Designing a Privacy-Aware Framework for Ethical Disclosure of Sensitive Data

Olusogo Joshua Popoola

A thesis submitted in partial fulfillment of the requirements of
Sheffield Hallam University
for the degree of Doctor of Philosophy

January 2025

Candidate Declaration

I hereby declare that:

1. I have not been enrolled for another award of the University, or other academic or Professional organisation, whilst undertaking my research degree.

2. None of the material contained in the thesis has been used in any other submission for an academic award.

3. I certify that this thesis is my own work. The use of all published or other sources of material consulted have been properly and fully acknowledged.

4. The work undertaken towards the thesis has been conducted in accordance with the SHU Principles of Integrity in Research and the SHU Research Ethics Policy, and ethics approval has been granted for all research studies in the thesis.

5. The word count of the thesis is **80,000**.

Name	Olusogo Joshua Popoola
Date	January 2025
Award	Ph.D.
Research Institute	Industry and Innovation Research Institute (I2R1)
Director(s) of Studies	Professor Alex Shenfield

Abstract

The increasing adoption of smart home healthcare ecosystems (SHHE) demands advanced privacy-preserving mechanisms to balance data utility with secure, ethical data disclosure. This thesis proposes a Privacy-Aware Authorization Framework that integrates a Dynamic Privacy Scoring Model (DPSM) and a Multi-Dimensional Dynamic Consent (MDDC) model within a decentralised smart contract infrastructure. This integration delivers context-aware, rule-enforced privacy decisions and decentralised, real-time consent enforcement with demonstrable accuracy, speed, and adaptability.

The first phase of implementation achieved high consent enforcement accuracy (99.8-99.9%), response times within benchmark (2.45s at peak load), and successful support for 15,000 concurrent requests with 99.3% delivery. User evaluations confirmed strong usability (SUS score of 85.2) and high confidence in system transparency and control. These outcomes validate the robustness of the DPSM and MDDC in enabling compliant, efficient, and user-centric privacy governance. To further enhance adaptability and precision, a machine learning-driven Privacy Violation Prediction Model (PVPM) was introduced. This model supported system optimisation through proactive anomaly detection and data-driven risk insights. Its integration into the framework enabled dynamic tuning of access rules and consent policies, resulting in an F1-score of 0.98 and an AUC of 0.9976, confirming its value in mitigating evolving privacy threats and reducing manual intervention.

This work contributes a scalable, adaptive privacy framework that harmonises mathematical scoring, user-centric consent, and intelligent automation. The proposed system establishes a benchmark for privacy-preserving design in SHHE while offering broader applicability to sectors requiring sensitive data control. Future research will explore advanced privacy-preserving techniques, including bio-authenticated dynamic consent, privacy-preserving federated learning, and quantum-resistant security models to address emerging threats while extending applications to multi-domain environments requiring sensitive data control.

Keywords: Smart Home Healthcare Ecosystem (SHHE), Dynamic Privacy Scoring Model (DPSM), Multi-Dimensional Dynamic Consent (MDDC), Privacy Violation Prediction Model (PVPM), Machine Learning for Privacy, Blockchain-Based Smart Contracts.

Publications and Manuscripts

The research work presented in this thesis has produced the following publications and manuscripts:

Published Articles

1. **Popoola, O**., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehia, A., & Popoola, J. (2023). A Critical Literature Review of Security and Privacy in Smart Home Healthcare Schemes Adopting IoT & Blockchain: Problems, Challenges and Solutions. *Blockchain: Research and Applications,* Volume 5, Issue 2, June 2024, 100178. https://doi.org/10.1016/j.bcra.2023.100178.

2. **Popoola, O**., Rodrigues, M. A., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). An Optimized Hybrid Encryption Framework for Smart Home Healthcare: Ensuring Data Confidentiality and Security. *Internet of Things; Engineering Cyber Physical Human Systems*, Volume 27, October 2024, 101314. https://doi.org/10.1016/j.iot.2024.101314

3. Tanimola, O., Shobayo, O., **Popoola, O**., & Okoyeigbo, O. (2024). Breast Cancer Classification Using Fine-Tuned SWIN Transformer Model on Mammographic Images. *Analytics*, *3*(4), 461-475. https://doi.org/10.3390/analytics3040026

Manuscripts Under Review

3. **Popoola, O**., Shenfield, A., Marchang, J., Ikpehai, A., Rodrigues, M., & Popoola, J. Leveraging Smart Contract-Based Access Control for Enhanced Data Ownership, Autonomy, and Privacy in Healthcare IoT Systems. Submitted to *Computer Standards & Interfaces*. Manuscript Number: CSI-D-24-00734 (Under Review)
   PDF Built of the manuscript at submission: https://shorturl.at/VVJwb
   Non-peer-reviewed by SSRN available on:
   https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4997749

4. **Popoola, O**., Shenfield, A., Marchang, J., Ikpehai, A., Rodrigues, M., & Popoola, J. "Machine Learning-Enhanced Blockchain for Healthcare IoT: Optimizing Data Privacy, Ownership, and Utility." Submitted to *Blockchain: Research and Applications*. Manuscript Number: BCRA-D-24-00593 (Under Review).
   PDF Built of the manuscript at submission: https://shorturl.at/E6xdD

5. **Popoola, O**., Shenfield, A., Marchang, J., Ikpehai, A., Rodrigues, M., & Popoola, J. "Temporal Privacy Elasticity and User Preferences in Smart Home Healthcare: A Cross-

Generational Analysis for Privacy-Aware Systems." Submitted to *International Journal of Human-Computer Studies*. Manuscript Number: IJHCS-D-24-01177 (With Editor)

PDF Built of the manuscript at submission: https://shorturl.at/65HcW
Non-peer-reviewed by SSRN available on:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5008167

6. **Popoola, O**., Shenfield, A., Marchang, J., Ikpehai, A., Rodrigues, M., & Popoola, J. "Understanding User Acceptance and Privacy Preferences in Smart Home Healthcare: Survey-Based Evaluation of the P-ASSHE System." Submitted to *Computers in Human Behavior*. Manuscript Number: CHB-D-24-05477 (With Editor)

   PDF Built from the manuscript at submission: https://shorturl.at/Ca08w

The content of these publications and submitted manuscripts form integral parts of various chapters in this thesis.

Acknowledgement

First of all, I would like to express my profound gratitude to my Director of Studies, Prof. Alex Shenfield (present) and Prof. Marcos Rodrigues (past), for their guidance, research freedom, robust critique, invaluable learning opportunities, and constant support. I am also deeply thankful to my supervisory team, Dr. Jims Marchang, Dr. Augustine Ikpehai, and Rapporteur-Dr. Carlos Eduardo da Silva, for providing valuable feedback and suggestions throughout my research journey. I further extend my sincere appreciation to my thesis examiners, Dr. Tooska Dargahi and Prof. Reza Saatchi, for their thorough evaluation and insightful comments that helped refine the final quality of my thesis. Working with all of them has been both an honour and a pleasure.

I am very grateful to the Industry and Innovation Research Institute (I2RI) at SHU for fostering a thriving research environment. The knowledge, experience, discussions, research events, and consortium for collaboration and training opportunities they provided have greatly expanded my knowledge in this field. I also gratefully acknowledge the partnership of the Tertiary Education Trust Fund (TETFund) and the University of Ilorin, Nigeria for providing the funding for my PhD program.

I sincerely thank the academic and support staff of the School of Computing and Digital Technologies for their invaluable contributions to my research journey. I thank you Richard Johnson for supporting me on the testbed equipment and setups. Likewise, I thank the leadership of the Department of Computing Engineering, University of Ilorin for their unwavering support throughout my course of study.

Furthermore, I am deeply thankful to my lab mates and colleagues at SHU for their friendship, support, and stimulating discussions that helped me through stressful situations and kept me motivated. Working with you all has been an unforgettable and rewarding experience.

Special thanks to my family, Dr. Jumoke Popoola (Wife), Esther, Nathan, and Eniola (Children) for their understanding, constant support, love, and encouragement. Your support throughout this great journey has been invaluable. Likewise, I appreciate the love and support from my siblings.

I want to thank my friends, Tunde, Ade, Seun, and Dan (to mention just a few) for standing by me. You are truly God-sent and friends indeed!

Contents

List of Figures

List of Tables

List of Abbreviations

AAL	Ambient Assisted Living
ABAC	Attribute-Based Access Control
AES	Advanced Encryption Standard
AI	Artificial Intelligence
BAADS	Blockchain-Aware Anomaly Detection Score
BCT	Blockchain technology
CBAC	Capability-Based Access Control
CCPA	California Consumer Privacy Act
CEF	Computational Efficiency Factor
CNN	Convolutional Neural Network
DSF	Data Sensitivity Factor
DPUTS	Dynamic Privacy-Utility Trade-off Score
DPSM	Dynamic Privacy Scoring Model
EHR	Electronic Health Record
ECC	Elliptic Curve Cryptography
HEN	Hardhat Ethereum Network
HIPAA	Health Insurance Portability and Accountability Act
IG	Information Gain
IoT	Internet of Things
IoHT	Internet of Health Things
IoMT	Internet of Medical Things
IPFS	InterPlenatary File System
GDPR	General Data Protection Regulation
LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, and Non-compliance
LSTM	Long Short-Term Memory

NIST	National Institute of Science and Technology
MI	Mutual Information
ML	Machine Learning
MDDC	Multimedia Dimensional Dynamic Consent
PARROT	PrivAcy by design tool foR inteRnet Of Things)
P-ASSHE	Privacy-Aware Smart Home Healthcare Ecosystem
PETs	Privacy Enhancing Technologies
PHI	Personal Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act
PL	Privacy Loss
PPUM	Privacy-Preserving Utility Metric
PVPM	Privacy Violation Prediction Model
RBAC	Role-Based Access Control
RBWF	Role-Based Weight Factor
RPM	Remote Patient Monitoring
RSA	Rivest–Shamir–Adleman
SC	Smart Contract
SHHE	Smart Home Healthcare Ecosystems
SHS	Smart Home Systems
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
TDF	Time-Decay Factor
TSI	Temporal Stability Index

Chapter 1

1. Introduction

The Internet of Things (IoT) has emerged as a significant innovation in modern healthcare, connecting a vast network of uniquely identifiable devices capable of collecting data, self-organising, sharing resources, and adapting to environmental changes with or without human intervention (Kassab & Darabkh, 2020; Zhou, et al., 2021). IoT's promise in healthcare is particularly evident in smart home healthcare ecosystems (SHHE), which aim to improve the well-being and quality of life of vulnerable populations, such as the elderly and those with chronic conditions, who are aging in place or facing physical, emotional, or mental challenges (Majumder, et al., 2017).

A smart home is a residence equipped with IoT devices that can be automatically controlled, monitored, and accessed remotely, leveraging internet-connected devices to enable automation, integration, and intelligent remote management of systems. The Internet of Health Things (IoHT) has emerged, enabling well-being monitoring while also posing security challenges in data confidentiality and patient privacy (Rajasekaran, Maria, Rajagopal, & Lorincz, 2023). IoT architectures rely on fundamental components, such as the IoT Core, which play a crucial role in connecting, managing, and securing the vast network of devices.

The proliferation of IoT devices in SHHE has introduced significant privacy and security challenges. These challenges arise from the distributed nature of IoT networks, the sensitivity of the collected data, which often includes personally identifiable information (PII) and detailed insights into individuals' daily lives and health conditions (Neisse, Steri, & Nai-Fovino, 2017) and the lack of adequate access control mechanisms (Ogonji, Okeyo, & Wafula, 2020), which pose risks to user privacy and data confidentiality. In the context of SHHE, the privacy of users is of utmost importance, as these systems often involve the collection and processing of PII and health-related data (Firouzi, Chakrabarty, & Nassif, 2020). Entities within the SHHE, such as cloud storage databases and healthcare provider systems, are potential targets for cyber-attacks, which can lead to unauthorised access and privacy breaches (Newaz, Sikder, Rahman, & Uluagac, 2021).

The absence of fine-grained access control and the failure to consider data owners' consent compromises data ownership, autonomy, and privacy, leading to unauthorised access, data leakage, and potential misuse of sensitive information. These issues are not merely technical but also ethical, touching upon the fundamental rights of individuals to privacy and control over their data (Zyskind & Nathan, 2015).

To address these challenges, this research focuses on the concept of informed consent and ethical data management within SHHE. The goal is to shift the paradigm from a trust-based model to a control-based model that leverages a trustless data management architecture, where data owners have granular control over the access and utilisation of their sensitive information (Kolain & Wirth, 2018; Kshetri, 2017). By prioritising user consent and providing a consent-centric privacy model-driven approach, this study aims to ensure the ethical disclosure of sensitive data and protect user privacy in SHHE. This approach addresses the lack of data sovereignty and provenance, which often results in unethical disclosure of sensitive data and denial of privacy, by implementing a fine-grained access control mechanism through a consolidated publisher-subscriber smart contract.

This balance between data protection and necessary sharing aligns with Acquisti (2010) observation that *"Solving the privacy problem means to find a balance between information sharing and information hiding that is in the best interests of data subjects but also of society as a whole" (p. 42).* The proposed framework operationalises this balance by employing granular access controls, which restrict data access to authorised entities based on well-defined criteria, and consent-driven mechanisms, which empower data subjects to define how their information is shared and used.

In the rest of this chapter, this work provides the background study on smart home healthcare data management systems and how they typically operate, with a specific focus on user privacy preservation. It explains how the work in this thesis relates to them and motivates its value with excerpts from relevant literature. The main objectives and contributions are listed, and an overview of the rest of the thesis is given.

1.1 Background and Problem Statement

The rapid proliferation of Internet of Things (IoT) devices has significantly transformed various application domains, including smart home healthcare ecosystems (SHHE). These ecosystems leverage IoT-enabled devices for real-time health monitoring, automated assistance, and data-driven decision-making to improve patient outcomes and quality of life. However, the integration of IoT in healthcare environments introduces critical privacy and security challenges, particularly concerning unauthorised access, unethical disclosure, and data leakage of sensitive health information.

These challenges stem from the inherent nature of IoT architectures, which involve a multitude of interconnected devices collecting, processing, and transmitting sensitive personal and health-related data. Thus, compromised IoT devices, unauthorised access to PII, and data owners' inability to selectively disclose their information have led to concerns of indiscriminate exposure of sensitive and contextual information. This growing vulnerability of personal information aligns with Holvast (2009) prescient observation and reiterated by Keulen and Kroeze (2018) that *"We must conclude that we are increasingly going to live in a surveillance society in which almost everything about our lives will be known"(p. 14).* Indeed, this surveillance risk is further amplified by the heterogeneous environment of IoT systems, which contributes to security and privacy challenges encountered in SHS (Ali et al., 2017; Bugeja et al., 2016).

To mitigate these risks, a robust privacy-aware architecture is necessary to ensure secure data flow, seamless device communication, and context-aware access control. It is therefore essential to examine the architecture that ensures secure data flow, efficient device communication, and seamless integration of IoT systems. In this context of this study, the IoT core components which represent the foundational infrastructure responsible for enabling the interaction between devices, securing data exchange, and ensuring seamless communication are investigated. Similar to the traditional computing architectures or even the proprietary service offered by AWS IoT Core, the IoT ecosystems examined in this study are characterised by heterogeneous, distributed environments, where privacy risks arise at multiple levels, including data collection, processing, integration, transmission, storage, security enforcement (access control) and monitoring. The IoT core, comprising six essential components i.e., Device Registry, Security, Messaging, Integrations, Edges, and Monitoring, plays a pivotal role in managing and securing these interactions. Each component introduces distinct privacy

vulnerabilities, particularly in SHHE, where data flows across multiple stakeholders such as patients, caregivers, healthcare providers, and research institutions.

In privacy-critical applications such as SHHE, where real-time patient data is collected and shared with multiple stakeholders, the IoT core components introduce unique privacy vulnerabilities. The primary privacy concerns associated with the IoT core in smart home healthcare ecosystems include:

1. Uncontrolled Data Collection (Device Registry)
    - The continuous logging of patient health metrics (e.g., heart rate, activity levels) by low-end IoT devices raises concerns about excessive data exposure without explicit user control.
    - Lack of fine-grained consent mechanisms leads to unauthorised data processing, creating risks of privacy violations.
2. Weak Access Control & Data Exposure (Security)
    - IoT security frameworks often rely on static access control models, failing to dynamically adapt to evolving privacy risks in SHHE.
    - Inadequate encryption and authentication mechanisms expose patient records and real-time health monitoring data to security breaches.
3. Insecure Data Transmission & Notification (Messaging)
    - The notification of collected data (e.g., patient vitals sent to healthcare professionals) lacks transparency mechanisms, increasing the risk of data interception and unauthorised access.
    - Lack of end-to-end encryption in device-to-device or device-to-cloud communications exposes sensitive information to man-in-the-middle attacks.
4. Interoperability Risks in Data Integration (Integrations)
    - IoT-enabled healthcare requires seamless data exchange across multiple stakeholders (hospitals, insurers, research bodies), but unregulated third-party integrations introduce privacy leakage risks.
    - Poorly designed integration protocols may allow cross-platform data sharing without user consent, violating regulatory compliance (e.g., GDPR, HIPAA).
5. Edge Computing Privacy Risks (Edges)
    - High-end IoT devices that perform on-device data processing reduce latency but may store unencrypted health records locally, increasing the attack surface.

- Edge-based analytics lacks standardised privacy-preserving mechanisms, leading to the potential unauthorised profiling of patients.

6. Insufficient Data Oversight & Transparency (Monitoring)
    - The lack of comprehensive audit trails in monitoring IoT-enabled SHHE limits users' ability to track data usage, making it difficult to detect policy violations or data misuse.
    - The absence of automated consent revocation mechanisms means patients cannot efficiently manage their privacy preferences in real time.

Figure 1.1 illustrates how these six components provide the key fundamental functionalities to form the IoT core, which serves as the primary layer for device connectivity, security enforcement, and data transmission within IoT-enabled environments (Arbaoui & Rahmoun, 2022; GeeksforGeeks, 2024; Ali et al., 2022). Table 1.1 further details each component's functionalities and real-world applications, particularly in smart home healthcare settings where data privacy and security are paramount.

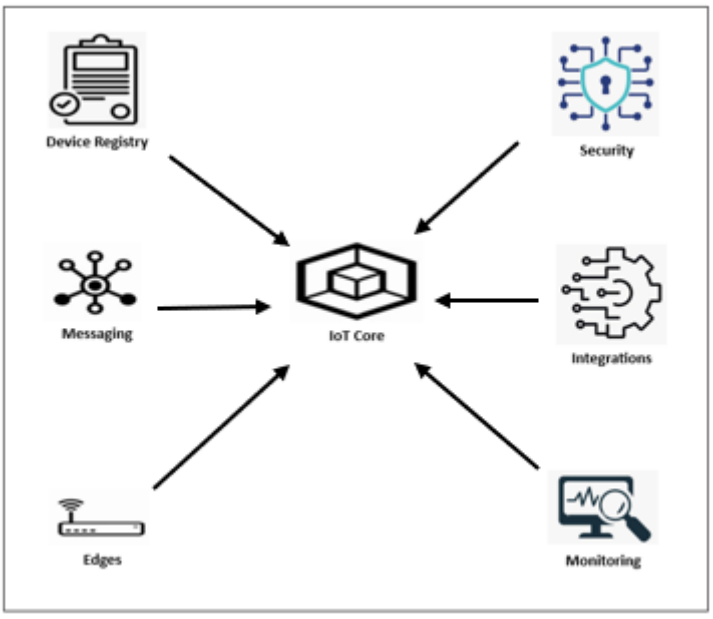


Figure 1. 1: IoT Core Components

Table 1. 1: IoT Core Components & Smart Home Healthcare Privacy Implications.

Component	Function	Privacy Challenges in Smart Home Healthcare
Device Registry	Registers IoT devices & manages identification.	Unregulated logging of patient data increases the risk of unauthorised monitoring.
Security	Implements authentication, authorisation, & encryption.	Weak access control compromises patient health data confidentiality.
Messaging	Facilitates real-time health data transmission.	Unencrypted data notifications expose sensitive health records.
Integrations	Connects external systems (EHRs, analytics, insurers).	Third-party data sharing risks violating patient consent.
Edges	Performs on-device data processing & analytics.	Local storage of sensitive data increases the attack surface.
Monitoring	Tracks device activity & access logs.	Lack of auditability prevents users from tracking data usage.

While Table 1.1 highlights the privacy challenges introduced by each IoT Core component, their combined interaction within a SHHE magnifies potential vulnerabilities. For instance, unencrypted messaging may inadvertently expose patient health data to unauthorized access, while a lack of interoperability in data integration could lead to fragmented access policies, causing compliance risks. These inherent vulnerabilities necessitate a structured, privacy-aware framework that integrates consent-centric authorization, adaptive access control, and real-time risk assessment to ensure secure data transmission and ethical information handling.

By implementing a security solution that effectively considers how to safeguard these core components from being compromised, this research lays the groundwork for a secure, privacy-aware, and efficient smart home healthcare ecosystems. The following paragraph examines the evolution of the smart home concept and its related technologies to provide further context.

As depicted in Figure 1.2, the rapid evolution of IoT-enabled environments has expanded the attack surface, heightening privacy risks (Butun, Sari, & Österberg, 2019). The transition from basic home automation to complex smart healthcare infrastructures has significantly increased data exposure vulnerabilities, necessitating a re-evaluation of privacy and security frameworks. The widespread adoption of IoT across sectors underscores the critical need for stricter data

protection measures, particularly in privacy-sensitive domains like healthcare. Addressing these challenges requires advanced privacy-preserving mechanisms, such as blockchain-based consent management, machine learning-driven anomaly detection, and fine-grained access control policies.

The SHHE exemplifies the growing privacy concerns associated with continuous IoT-enabled health monitoring. As the number of connected devices in SHHE increases, so does the complexity of securing personal health data. The risks include:

- Higher frequency of unauthorised access attempts due to increased network endpoints.
- Greater vulnerability to cyberattacks, such as data tampering & unauthorised profiling.
- Expanded legal & ethical challenges, requiring compliance with regulations like GDPR & HIPAA.

Thus, the IoT core should be contextually adapted to smart home healthcare by integrating privacy-enhancing measures such as privacy-preserving consent models, decentralised access control (smart contracts), and blockchain-based audit trails to mitigate the risks of unethical data disclosure.

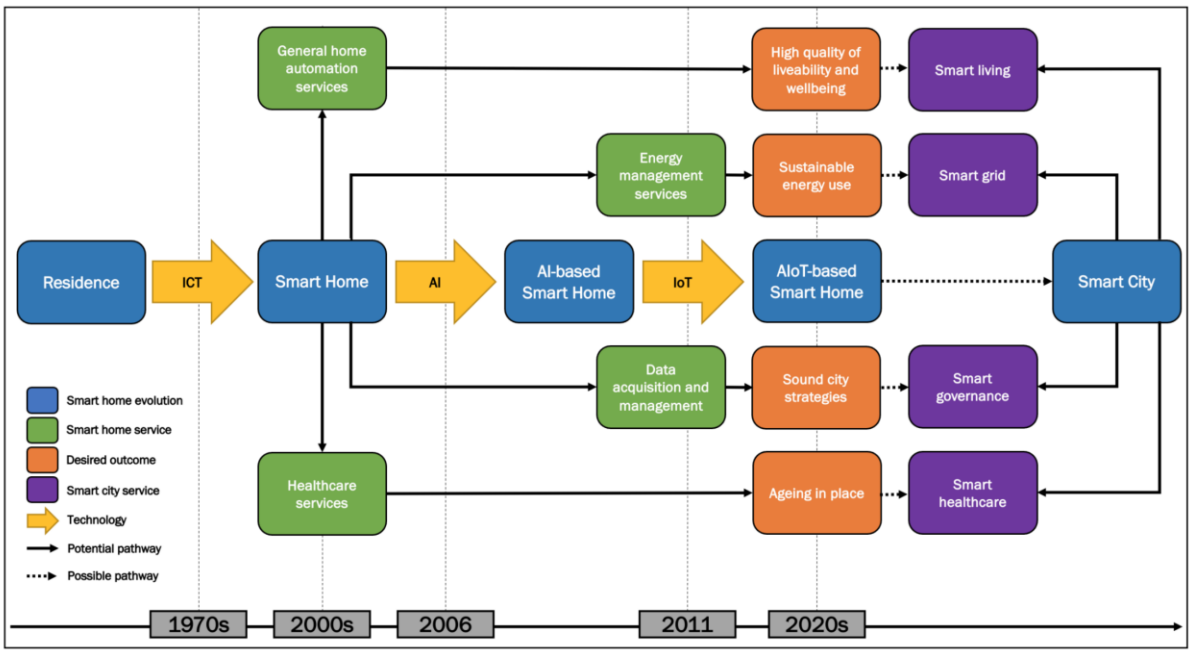


Figure 1. 2:Evolution Pathway of Smart Home Concept, Related Technologies, and Services (Source: Li, Yigitcanlar, Erol, & Liu, 2021).

As privacy norms dictate, data owners (users) should have control over their data, rather than complete withdrawal or non-disclosure (Popoola, et al., 2023; Sim, et al., 2023). Users should be able to selectively disclose information and exercise control over who sees it. However, privacy infringement can sometimes be acceptable when the disclosure of the information is beneficial to the data owner for the continuum of care. Intangible benefits of ethical disclosure of personal information could be for medical research, therapy logistics, design and well-being advertisement purposes. These processes should be supervised and controlled based on informed consent and acceptance (Pirzada et al., 2022), and the tenure of use as agreed by data owners (Dinev, et al., 2006; Kehr, Kowatsch, Wentzel, & Fleisch, 2015).

In the context of smart home well-being monitoring shown in Figure 1.3, both 'sensitive data' and 'private data' are highly relevant terms, and understanding their implications is crucial for data management, protection, and compliance with legal standards. Establishments behind the design and deployment of smart home devices are yet to employ strict data security measures and follow relevant regulations to ensure that both private and sensitive information are adequately protected against unauthorised access, disclosure, or other forms of data breaches.

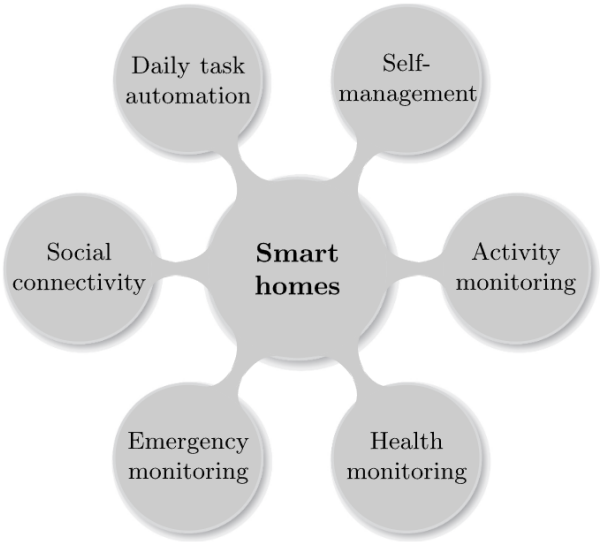


Figure 1. 3: Functionalities of a Smart Home Scenario Applicable for Well-being Monitoring (Source: Pirzada et al., 2022).

Existing smart home healthcare systems often lack adequate access control mechanisms for the ethical disclosure of sensitive data. The absence of fine-grained access control and the failure to consider data owners' consent compromises data ownership, autonomy, and privacy. This leads to unauthorised access, data leakage, and potential misuse of sensitive information,

highlighting the need for an authorisation framework that ensures the ethical disclosure of sensitive data through a consent-centric privacy model and smart contract-based access control.

1.2 Motivation and Purpose of the Study

The motivation for this research stems from the limited exploration of dynamic, consent-driven access control in SHHE and the insufficient focus on the components enabling such dynamism. While existing studies have addressed adaptive access control in IoT-based healthcare, they have not fully considered the specific factors driving real-time privacy adaptation or the context-sensitive mechanisms implemented in this study. Additionally, transparent and auditable data management remains an area requiring further refinement necessitating a privacy-preserving authorisation frameworks and consent-centric model that empowers data owners while ensuring ethical disclosure.

Studies indicate that assistive healthcare technologies are more widely accepted when they are customisable to individual needs (Chee, 2024; Kehr et al., 2015) and uphold user autonomy and dignity (Kumar et al., 2023; Schomakers & Ziefle, 2023). To address these limitations, this research proposes a smart contract-based, consent-centric privacy model that enables fine-grained access control through real-time privacy scoring. This approach integrates three core elements:

1. *Time-Decay Factor (TDF*) (λ) – Adjusts privacy scores over time to reflect evolving user preferences.
2. *Role-Based Weight Factor (RBWF)* (ω_r) – Ensures role-sensitive access control for stakeholders.
3. *Data Sensitivity Factor (DSF)* (γd) – Differentiates access permissions based on data classification.

The proposed model is designed to ensure:

- *Customisation and Control***:** Users define privacy preferences via smart contracts, tailoring access to their needs.
- *Dignity and Autonomy***:** Access is selectively granted, preserving user independence.
- *Seamless Integration***:** The system operates unobtrusively, fostering user acceptance.
- *Privacy Assurance***:** Dynamic access control mitigates unethical data disclosure.

The primary aim of this study is to develop a privacy-aware authorization framework that guarantees secure, ethical, and consent-driven data disclosure. This is demonstrated in Figure 1.4, which illustrates the data flow within the proposed framework.

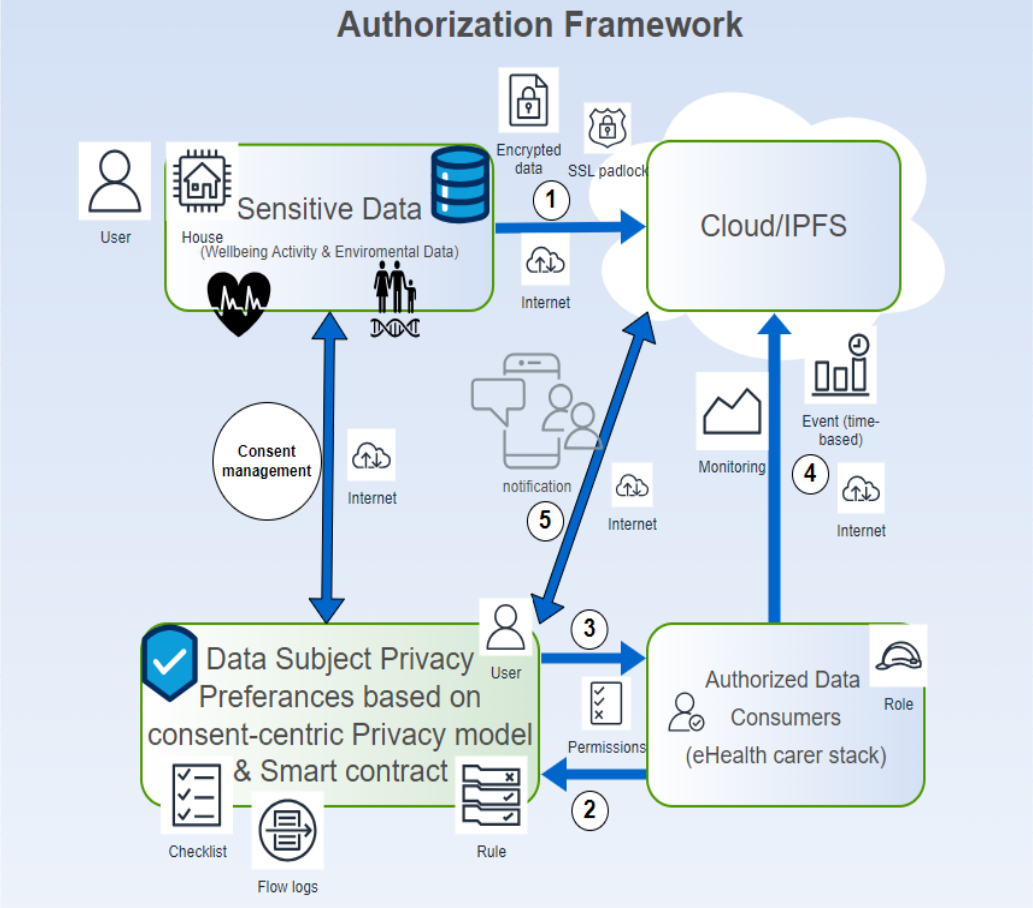


Figure 1. 4: Data Flow within the Proposed Authorisation Framework.

Legend:

1. **Upload**: Sensitive data from home sensors through the home gateway is sent to the cloud.
2. **Access Request**: Data consumers view access look-up via a role-based authorisation scheme.
3. **Grant Access**: Authorised data consumers are granted permission to view sensitive data based on smart contract-enabled consent-centric privacy preference of the data owner (home patient).
4. **Role-based** access to view data via **smart contract access control**.
5. **Transparency of data utility** via real-time notification of view events, including the ability to withdraw view access.

Dynamic Privacy Scorer

Authorised Data Consumer

The framework dynamically adjusts access control based on real-time privacy scoring, allowing data owners to revoke or modify consent preferences instantaneously. Additionally,

smart contracts enforce privacy-preserving policies in real-time, ensuring that access to sensitive data is granted only when predefined privacy conditions are met within the consent-centric model. The smart home healthcare ecosystem (SHHE) serves as the demonstration environment for this framework, encompassing:

- *Stakeholders*: Patients, healthcare providers, caregivers, family, research institute.
- *Technological Components*: IoT sensors, network devices, distributed ledger technology (DLT) for data integrity, and cloud storage for scalable, secure access.
- *Health Monitoring & Transparency*: Patients receive real-time updates, while stakeholders gain controlled access to sensitive data through immutable audit trails powered by DLT.

Beyond health monitoring, the proposed framework ensures transparent and accountable data access, addressing concerns about unauthorised use by healthcare providers, research institutes, and insurers. By leveraging smart contracts, access control is strictly enforced, protecting sensitive health data from unauthorised access and leakage, as depicted in Figure 1.5.

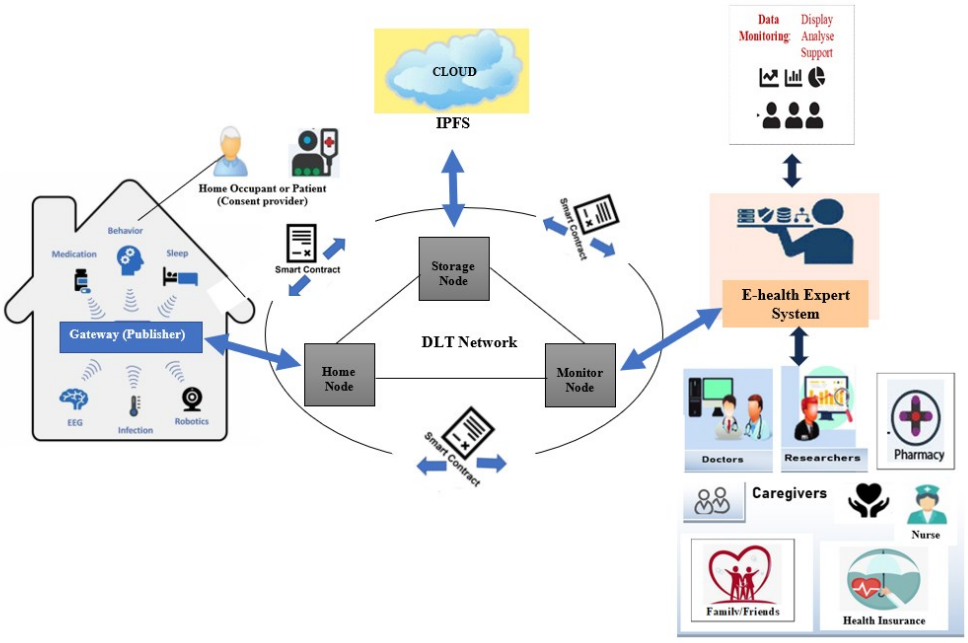


Figure 1. 5: The Smart Home Healthcare Stakeholders.

The proposed privacy-preserving framework for SHHE integrates key technological components i.e., IoT, blockchain, AI, and encryption, to provide a secure and adaptive access control system. IoT devices act as data generators, collecting real-time health information,

which is secured through encryption mechanisms during transmission. Blockchain technology ensures decentralised, immutable, and transparent access control by employing smart contracts for privacy enforcement. AI enhances this model by leveraging anomaly detection and dynamic privacy scoring, enabling real-time risk assessment and automated consent adaptation. These components collectively create a privacy-aware ecosystem where patient data is securely shared while maintaining granular access control based on real-time contextual privacy risks.

1.2.1 Research Aim

This study aims to develop a dynamic, privacy-aware authorisation framework that integrates IoT, blockchain, and AI-driven privacy risk assessment to enable secure, adaptive, and consent-centric access control for ethical disclosure of sensitive data in a smart home healthcare environment.

The research objectives, detailed in Section 1.3, include:

1. Investigating privacy and access control challenges in SHHE.
2. Developing a consent-centric privacy model.
3. Designing a smart contract-based access control mechanism.
4. Implementing and evaluating the framework in a simulated SHHE.

Chapters 3, 4, and 5 systematically address these objectives by covering the model's development, implementation, and evaluation.

1.3 Research Questions, Objectives, and Contributions

This research investigates privacy and security challenges in smart home healthcare ecosystems by integrating IoT, blockchain, and machine learning. The research questions (RQs) target core issues, while the objectives and contributions highlight novel frameworks and methodologies developed to address them.

1.3.1 Aligning Research Questions with Objectives and Contributions

RQ1:

What are the current privacy and access control challenges in smart home healthcare systems, and how can an adaptive, context-aware user interface be designed to address the gap between complex privacy requirements and user-friendly preference management?

Objective 1:

Investigate privacy and access control challenges in smart home healthcare systems and design an adaptive user interface that bridges the gap between technical privacy controls and user comprehension.

Contribution 1:

- Identification of gaps in current privacy models, informing the development of a consent-driven privacy model in subsequent research.
- Critical literature review (*Blockchain: Research and Applications, Popoola et al., 2023*) systematically categorising privacy challenges in SHHE.
- Implementation of a hybrid encryption framework (*Internet of Things: Engineering Cyber-Physical-Human Systems, Popoola et al., 2024*), ensuring data confidentiality and security in SHHE.

RQ2: How can a consent-centric privacy model be designed to address the limitations of static privacy controls and adapt to dynamic healthcare environments?

Objective 2:

Develop and validate a smart contract-based consent-centric privacy model integrating Dynamic Privacy Scoring Model (DPSM) and Multi-Dimensional Dynamic Consent (MDDC) to enable context-aware, ethical data disclosure.

Contribution 2:

- Design and implementation of DPSM and MDDC, adapting privacy controls to real-time user preferences, roles, and data sensitivity.
- Integration into a blockchain-based smart contract architecture, enabling self-executing, rule-based privacy enforcement in SHHE.
- Development of an adaptive, React-based front-end interface for intuitive privacy preference management via dynamic controls and real-time feedback mechanisms.
- Validation of security and privacy robustness through STRIDE and LINDDUN threat modeling, leveraging real-time security logs and simulated privacy threats (*under review in Computer Standards & Interfaces*).

Although adaptive rule-based frameworks enhance access control, they lack mechanisms to proactively predict privacy violations based on evolving access patterns. This limitation

necessitates the integration of machine learning-driven privacy risk assessment for predictive threat detection, ensuring real-time adaptation to potential privacy threats.

RQ3:
How can a machine learning-driven privacy risk assessment model enhance predictive risk awareness in smart home healthcare by learning access patterns and detecting privacy violations, thereby optimising the effectiveness of DPSM and MDDC for smart contract efficiency?

Objective 3:
Develop and integrate a machine learning-driven privacy preservation optimisation model for privacy risk violation assessment, addressing the absence of predictive privacy risk assessment in existing adaptive rule-based frameworks.

Contribution 3:

- Devised an ensemble-based privacy risk prediction model, combining Random Forest and Extra Trees classifiers to enhance risk classification and proactive anomaly detection.
- Refinement of the adaptive rule-based framework by incorporating privacy risk assessment to pre-emptively detect violations before access is granted.
- Empirical evaluation using real-world IoT healthcare data, including EHR access logs, anomaly detection records, and user consent datasets, with findings under review in *Blockchain: Research and Applications*.

RQ4:
How can quantifiable metrics for transparency and data integrity be developed to evaluate the effectiveness of the proposed authorisation framework in SHHE?

Objective 4:
Develop and implement comprehensive evaluation metrics assessing the framework's privacy preservation, transparency, security, and usability, ensuring practical applicability in real-world SHHE settings.

Contribution 4:

- Extensive performance evaluation, covering privacy, security, and user experience.
- User evaluation in SHHE, demonstrating usability effectiveness via System Usability Scale (SUS) of 85.2, confirming a highly acceptable user experience (*Section 6.3*).
- Beyond usability validation via the System Usability Scale (SUS) of 85.2, the framework's transparency and security were assessed through STRIDE/LINDDUN threat modeling and privacy impact analysis, confirming its robustness against unauthorised disclosures.
- Cross-generational privacy analysis, uncovering insights into privacy elasticity and shaping adaptive privacy frameworks (*findings under review in International Journal of Human-Computer Studies & Computers in Human Behavior*).

1.3.2 Overall Contributions of the Research

The proposed system introduces a dynamic, consent-centric privacy management framework, integrating temporal, role-based, and sensitivity factors within a smart contract-based access control scheme to enhance trust and stakeholder engagement. Additionally, Privacy Impact Assessment (PIA), in conjunction with LINDDUN and STRIDE threat modeling, is complemented by a machine learning-driven privacy risk assessment model, which leverages anomaly detection and predictive analytics to enhance privacy risk evaluation. By incorporating anomaly detection within the privacy risk assessment model, smart contracts dynamically adjust access permissions based on real-time risk factors, thereby enhancing the efficiency and responsiveness of access control in SHHE. This ensures proactive threat mitigation, regulatory compliance, and stakeholder confidence.

1.4 Thesis Overview

This thesis is divided into eight chapters, each contributing to the design of a privacy-aware authorisation framework for the ethical disclosure of sensitive data in smart home healthcare ecosystems.

Chapter 2 reviews recent advancements in privacy preservation, focusing on privacy-by-design principles, privacy-enhancing technologies, and access control mechanisms for IoT-driven environments.

Chapter 3 presents the methodology for ethical information disclosure, introducing a consent-centric privacy model that integrates time decay, data sensitivity, and stakeholder roles, with a mathematical model for computing dynamic privacy scores.

Chapter 4 presents the design of the authorisation framework, outlining the user and system requirements essential for its effectiveness and usability. It details the proposed integration of IoT devices, novel smart contract access control orchestration modeling within a permissioned blockchain network (HEN), ensuring that fine-grained, secure, and context-aware data transmission aligns with privacy preferences, role-based access policies, and real-time system constraints.

Chapter 5 focuses on the implementation and integration of the authorisation framework within the smart home healthcare ecosystem, including the role-play of stakeholders.

Chapter 6 presents the testing, validation, and user evaluation of the framework, assessing its resilience, privacy score effectiveness, and usability through agile prototyping and user-centric evaluation.

Chapter 7 explores machine learning-driven privacy preservation and system optimisation, emphasising adaptive privacy risk assessment, anomaly detection, and real-time privacy-utility trade-off optimisation.

Chapter 8 concludes the thesis by summarising how research objectives were achieved, highlighting contributions to the body of knowledge, and identifying future research directions.

Chapter 2

2. Literature Review

Several studies in the field of smart home security exist, mostly focusing on challenges experienced by vendors, implementers, and users when adopting the IoT in smart homes, and measures taken to address them. Emerging research has proposed various stand-alone architectures and frameworks to secure IoT devices in smart homes while others proposed a combination of technologies to enhance the security of devices and guarantee data protection; with issues around device, communication, service, and applications connected to devices identified as areas where the main security and privacy challenges in smart connected homes are experienced (Bugeja et al., 2016; Ali et al., 2017). Moreover, several papers discuss common security issues of IoT-enabled smart homes such as privacy, inter-compatibility, authentication, and secure end-to-end connection in the presence of adversarial behaviour, and argue that secure end-to-end cryptographic framework could be the elusive panacea.

The National Institute of Science and Technology (NIST) proposed a privacy framework stating five core functionalities for achieving data privacy in the study by Lefkovitz and Boeckl (2020), which include data control, communication, identification, governing data, and data protection. It was further argued that privacy could be defined as freedom from intrusion and possession of the ability to control personal data, while security refers to data protection against unauthorised access to user data (Mazumdar & Dreibholz, 2022). Some even go as far as relating "Confidentiality" (a property of data) to "Privacy" (a property of an individual). Moreover, Boehme-Neßler (2016) stated, *"Privacy is not only an arbitrary cultural and legal concept. It is an anthropological constant and a psychological necessity. It is a complex process of selectively managing access to one's self. Without a minimum of privacy people can't survive" (p. 222).*

In handling privacy issues, all phases of the data value chain must be considered, including acquisition/collection, analysis, storage, and usage. Two practical solutions to address these challenges are implementing privacy by design (Barth, 2021) and using privacy-enhancing technologies (D'Acquisto et al., 2015). Techniques often discussed to ensure privacy as illustrated in Figure 2.1 include:

i). Security, encryption, anonymisation, and accountability controls (e.g., data provenance, policy enforcement, granular access control, accountability, and auditability).

ii). Ownership, consent management, transparency, and control (e.g., privacy preferences, consent, sticky policies, personal data stores).

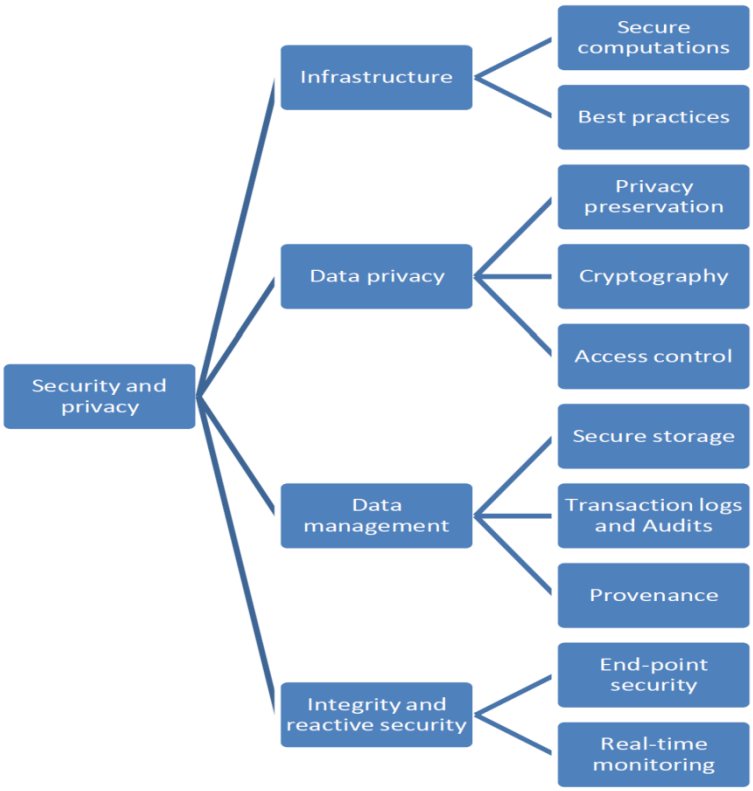


Figure 2. 1: Security and Privacy Taxonomy

2.1 Overview of Smart Home and Smart Healthcare Ecosystems

The integration of smart home technologies with healthcare services has led to the development of ecosystems that significantly enhance the quality of life, especially for the elderly and those with chronic health conditions (Pirzada et al., 2022). This section provides an overview of the evolution of smart home technologies, the components that constitute these systems, the advancements in smart healthcare technologies, and the integration of these two domains into a cohesive ecosystem.

2.1.1 Evolution of Smart Home Technologies

Smart home technologies have evolved significantly from their inception, transitioning from simple home automation systems to complex networks of interconnected devices, sensors, and systems designed to enhance the comfort, convenience, and efficiency of residential spaces (D'Acquisto et al., 2015; Becher, Gerl, Meier, & Bölz, 2020). At its core, a smart home leverages IoT technology to enable seamless communication and coordination among various household appliances, environmental controls, and security systems (Yan et al., 2022).

Initially, smart homes primarily focused on automating household tasks such as lighting, heating, and security. These early systems relied heavily on wired networks and were often expensive and difficult to install. However, advancements in wireless communication, sensor technologies, and IoT have dramatically transformed smart homes into more accessible and sophisticated environments. This integration of technologies aims to create intelligent living environments that adapt to residents' needs and preferences, offering an improved quality of life, particularly for older adults and individuals with special needs (Al-Kahtani, Khan, & Taekeun, 2022; Majumder, et al., 2017).

Central to the smart home ecosystem is the home automation system, which serves as the brain of the network by processing data from multiple sources and executing commands based on predefined rules or user preferences (Bansal & Kumar, 2020). Modern smart homes now incorporate a wide range of IoT devices, including smart thermostats, security cameras, lighting systems, home entertainment systems, and remote monitoring services.

This system typically includes a central hub or gateway that facilitates communication between different devices and protocols, ensuring interoperability between products from various manufacturers (Famá, Faria, & Portugal, 2022). For example, devices interconnected through wireless protocols such as Wi-Fi, Zigbee, and Z-Wave enable seamless communication and automation. The integration of Artificial Intelligence (AI) and Machine Learning (ML) further enhances the capabilities of smart homes, enabling predictive maintenance, energy management, and personalised user experiences (Psychoula, 2020).

The market for smart home technologies has experienced substantial growth, driven by the increasing demand for convenience, energy efficiency, and security, as well as the growing aging population and rising demand for home healthcare and ambient assisted living. The IoT market has expanded significantly, from over 15 billion devices in 2016 to a projected 75

billion worldwide by 2025 (Statista; Butun, Sari, & Österberg, 2019). This figure encompasses all active connections and excludes devices that were previously purchased but are no longer in use. Consequently, the average smart home is anticipated to host more than 50 internet-connected devices by 2025.

According to recent industry projections, the global smart home market is expected to grow from £75.80 billion in 2023 (Insights, 2024) to around £130.68 billion by 2025, reflecting a compound annual growth rate (CAGR) of approximately 13.52% during this period (Research, 2018). This growth highlights the expanding adoption of smart home technologies across various demographics, underscoring the increasing integration of these technologies in everyday life, particularly for elderly care and assisted living (D'Acquisto, et al., 2015). The rise of consumer smart home platforms and connected devices empowers users to establish their own automated IoT environments. To offer personalised services, these systems are enabled to gather sensitive personal data, such as vital signs, medical records, location, and behavioural patterns.

However, the proliferation of connected devices in the home also introduces new challenges. Data privacy and security concerns are paramount, as the vast amount of personal information collected by these devices could be vulnerable to breaches or misuse (Sivakumar, Mone, & Abdumukhtor, 2024). Additionally, the lack of standardisation across different manufacturers can lead to interoperability issues, potentially limiting the seamless integration of devices from various brands (Sousa, Mendonça, & Machado, 2022; Egala, Pradhan, Badarla, & Mohanty, 2021). Consequently, continuous monitoring poses privacy and security risks, necessitating the creation of Privacy Enhancing Technologies (PETs) (Schomakers & Ziefle, 2023) that suggests several solution directions including the use of resilient application layers that safeguard against runtime attacks. These environments leverage cryptographic enhancements to ensure data security, such as improved stream ciphers for securing IoT device communications (Mahdi, Hassan, & Abdul-Majeed, 2021).

2.1.2 Components of Smart Home Systems

A typical smart home system integrates several key components to deliver a cohesive and automated living environment. *IoT devices*, such as sensors, actuators, and smart appliances, play a central role by collecting data and executing commands. Examples include smart thermostats, lighting systems, security cameras, and health monitoring devices (Chakraborty,

et al., 2023). These devices communicate through a *home gateway*, which connects various IoT devices within the home to the internet, facilitating remote access and control while bridging different communication protocols (Rahimi, Songhorabadi,, & Kashani, 2020; Pavlović, et al., 2022). The collected data is often processed and stored on *cloud platforms*, which provide computational resources for advanced analytics and machine learning to derive actionable insights (Yassine, Singh, Hossain, & Muhammad, 2019).

Interaction with the smart home system is made seamless through intuitive *user interfaces*, such as mobile apps, web dashboards, and voice-activated assistants like Amazon Alexa and Google Home, allowing users to control devices and receive notifications (Ceccacci & Mengoni, 2017). All these elements depend on a robust *network infrastructure* that ensures reliable communication between IoT devices, gateways, and cloud services using technologies such as Wi-Fi, Bluetooth, and Zigbee (Fox, Donnellan, & Doumen, 2019). Together, these components form the foundation of a smart home ecosystem, enabling personalised care and remote health monitoring e.g., Ambient Assisted Living (AAL) solutions, particularly when integrated with healthcare technologies.

2.1.3 Overview of Smart Healthcare Technologies

Smart healthcare technologies have advanced significantly, aiming to improve patient care and management, particularly for chronic diseases and elderly care. These technologies leverage IoT, wearable devices, and mobile health applications to provide real-time monitoring and data collection and early detection of potential health issues, thereby enhancing the delivery of healthcare services (Mahmmod, et al., 2024). Moreover, the smart healthcare environment represents a paradigm shift in the delivery of healthcare services, leveraging advanced technologies to create a more efficient, personalised, and proactive approach to patient care (Sripathi & Leelavati, 2024). This ecosystem integrates various components of healthcare delivery, including medical devices, information systems, and communication technologies, to enable seamless data exchange and improved decision-making processes (Mbunge, Muchemwa, & Batani, 2021).

At the heart of the smart healthcare ecosystem is Internet of Medical Things (IoMT) devices, which include wearable health trackers, implantable sensors, and smart medical equipment (Ahmed, et al., 2024). These technologies enable critical innovations in healthcare delivery,

focusing on personalization and efficiency. *Wearable health devices*, such as smartwatches and fitness trackers, monitor vital signs like heart rate, blood pressure, and activity levels, providing real-time health data to users and healthcare providers. These devices are essential for continuous health monitoring, facilitating timely interventions, and personalized care (Luo, Tan, & Wen, 2024). Similarly, *remote patient monitoring (RPM)* systems collect real-time health data from patients and transmit it to healthcare providers, enabling proactive management of chronic conditions such as diabetes and hypertension. This approach allows for continuous monitoring and timely healthcare interventions, particularly beneficial in reducing hospital readmissions (Boikanyo, Zungeru, Sigweni, Yahya, & Lebekwe, 2023).

Telemedicine extends these capabilities by facilitating remote consultations between patients and healthcare professionals, reducing the need for in-person visits and improving access to medical services. Its relevance has grown significantly during the COVID-19 pandemic, enabling patients to receive care while minimising exposure risks. Integrated with smart home technologies, telemedicine also supports early intervention and remote monitoring of patient's health statuses (Kaundinya & Agrawal, 2022) (Conley, Snyder, Whitehead, & Levine, 2022). Additionally, *electronic health records (EHRs*) play a critical role in this ecosystem, serving as centralised repositories for patient data. By digitising health records, EHR systems enable seamless information sharing among healthcare providers, improving care coordination, reducing medical errors, and incorporating predictive analytics for advanced decision-making (Rogers, Parulekar, Malik, & Torres, 2022; Hernandez, 2021; Giordano, et al., 2021).

Moreover, health analytics and artificial intelligence (AI), including machine learning (ML), are transforming healthcare by enhancing diagnostic accuracy, personalising treatments, and improving operational efficiency (Sahu, Gupta, Ambasta, & Kumar, 2022). AI-driven solutions have revolutionized healthcare delivery, enabling data-driven insights and advanced predictive capabilities. For instance, AI-powered imaging tools assist radiologists in detecting abnormalities more accurately and efficiently, while ML algorithms predict patient outcomes using vast datasets of historical health records (Oyeniyi & Oluwaseyi, 2024; Vanaparthi & Rao, 2023; Rana & Shuford, 2024).

Despite the numerous benefits, the smart healthcare ecosystem also faces significant challenges. Data privacy and security concerns are paramount, given the sensitive nature of health information (Jaime, Muñoz, Rodríguez-Gómez, & Jerez-Calero, 2023). Ensuring

interoperability between different systems and devices remains a challenge, as does the need for robust cybersecurity measures to protect against potential breaches (Argaw, et al., 2020). Additionally, there are ethical considerations surrounding the use of AI in healthcare decision-making and the potential for algorithmic bias (Osasona, et al., 2024). The digital divide also poses a challenge, as not all patients have equal access to the technologies that enable smart healthcare (Khilnani, Schulz, & Robinson, 2020).

Recently, Blockchain technology has emerged as a potential solution to address data security and interoperability challenges in the smart healthcare ecosystem (Jabbar, Fetais, Krichen, & Barkaoui, 2020; Popoola O. , et al., 2023). By providing a decentralised and tamper-resistant ledger for health data, blockchain can enhance data integrity, facilitate secure data sharing, and give patients greater control over their health information (Lavanya & Kavitha, 2022; Egala, Pradhan, Badarla, & Mohanty, 2021).

As the smart healthcare ecosystem continues to evolve, there is a growing focus on patient-centric approaches that empower individuals to take a more active role in managing their health (Chibuike, Sara, & Adele, 2024; Aminabee, 2024; Toni, Mattia, & Pratesi, 2024). More so when the severe and worsening shortage of healthcare workers, combined with the increasing number of elderly and chronically ill individuals, is affecting the capacity of health systems, particularly in industrialised countries, to deliver safe and cost-effective services for older adults (Demiris & Thompson, 2011). This aligns closely with the principles of ambient assisted living, where smart home technologies are integrated with healthcare solutions to support independent living and improved quality of life for older adults and individuals with chronic conditions.

The integration of smart homes and smart healthcare ecosystems presents both opportunities and challenges, particularly in terms of privacy and data protection. The following section will explore this integration in more detail, examining the potential benefits and privacy considerations that arise in this convergence.

2.1.4 Integration of Smart Home and Healthcare Ecosystems

The integration of smart home and healthcare ecosystems, referred to as smart home healthcare ecosystems, represents a significant advancement in personalised healthcare and Ambient

Assisted Living (AAL). This convergence combines home automation with health monitoring, creating a comprehensive environment that enhances proactive health management and quality of life, particularly for older adults and individuals with chronic conditions (Wróbel-Lachowska, et al., 2023; Bidgoli, 2023). Central to this integration is the use of healthcare-specific sensors and devices, such as smart floors that detect falls or smart medication dispensers that ensure adherence to prescriptions (Ahmad, et al., 2022; Davis, Kirwan, Maclay, & Pappas, 2022). These technologies, coupled with wearable health devices and IoT medical sensors, enable continuous health monitoring and provide a comprehensive picture of an individual's well-being within their living environment (Mohammed, Desyansah, Al-Zubaidi, & Yusuf, 2020; Morita, Sahu, & Oetomo, 2023).

The integration of these systems offers numerous benefits. Continuous health monitoring through smart sensors and devices provides an unobtrusive way to track vital signs and detect anomalies in real-time, enabling early interventions and potentially preventing hospitalisations (Mohammed, Desyansah, Al-Zubaidi, & Yusuf, 2020; Morita, Sahu, & Oetomo, 2023). Enhanced safety and security are achieved through features like emergency response systems and automated alerts, which are particularly beneficial for elderly individuals living independently (Wang, Grundy, Khalajzadeh, Madugalla, & Obie, 2024). Additionally, improved communication between patients, caregivers, and healthcare providers ensures better care coordination by providing all stakeholders with access to up-to-date health information (Gall, et al., 2022). These systems also facilitate personalized care by leveraging data from health monitoring devices and smart home technologies to tailor healthcare interventions and lifestyle recommendations to individual needs (Siddiqui, Khan, & Dey, 2022). As a result, these integrated systems significantly enhance users' independence, enabling them to manage daily tasks more effectively while receiving the necessary support (Aggar, Sorwar, Seton, Penman, & Ward, 2023; Rock, Tajudeen, & Chung, 2024)

Despite these advancements, integrating smart home and healthcare systems presents significant challenges, particularly concerning privacy and security. The collection and use of sensitive health data require compliance with stringent regulations such as GDPR and HIPAA. Ensuring appropriate data classification and handling within these systems is complex, as the combination of health and non-health data introduces risks of misclassification and potential misuse (Houser & Bagby, 2023; Tzanou, 2023). Data ownership and control further complicate this ecosystem, as the ambiguity surrounding ownership in multi-device

environments raises questions about access rights and permissions (Chen, Edwards, Urquhart, & McAuley, 2020; Asswad & Marx Gómez, 2021). Effective consent management is also critical, given the pervasive and dynamic nature of data collection in these systems. Developing mechanisms that allow users to provide, modify, and withdraw consent without inducing fatigue remains a key challenge (Carroll, et al., 2020; Azodo, Williams, Sheikh, & Cresswell, 2020). Furthermore, data segmentation is essential to distinguish health-related data from other types, as improper classification can lead to unnecessary exposure or insufficient protection (Psychoula, et al., 2018).

Interoperability and security are additional areas of concern. Ensuring secure communication between devices requires standardisation and robust protocols to prevent data breaches and inconsistencies (Lee, Seo, Oh, & Kim, 2021). Poor device compatibility and vulnerabilities in communication protocols exacerbate these issues, necessitating custom configurations that may introduce further risks. To address these challenges, researchers and industry leaders are exploring solutions such as edge computing for local data processing, blockchain-based architectures for secure data sharing, and user-centric interfaces for enhanced control over data (Osman, Taiwo, Elashry, & Ezugwu, 2023; Malik & Shah, 2022). Ethical governance frameworks are also critical for addressing issues like algorithmic bias in health predictions and ensuring equitable access to these technologies (Murphy, et al., 2022). Balancing the immense benefits of these integrated systems with robust privacy and security measures remains a critical area of research and development.

2.2 Privacy and Security Challenges in Smart Home Healthcare

The integration of smart home technologies with healthcare services has significantly enhanced the quality of life for many individuals, particularly the elderly and those with chronic conditions. However, this integration also introduces substantial privacy and security challenges that must be addressed to ensure the safety and trust of users. Moreover, as these systems collect, process, and transmit sensitive data, ensuring the confidentiality, integrity, and availability of this information becomes paramount. Hence, the need to duly explore the key privacy and security challenges in SHHE including various threats, vulnerabilities, and potential impacts on users.

2.2.1 Privacy Issues in Smart Home Environments

Smart home environments collect vast amounts of personal data through various IoT devices, including sensors, cameras, and health monitoring tools (Vardakis, Hatzivasilis, Koutsaki, & Papadakis, 2024). This data can include sensitive information about an individual's daily routine, habits to vital signs and medication schedules, health status, personal preferences, and environmental data (Dhanraj, et al., 2024). The aggregation and analysis of this data can lead to significant privacy concerns, particularly if the data is accessed or used without the individual's consent (Rivadeneira, Silva, Colomo-Palacios, Rodrigues, & Boavida, 2023).

Table 2.1 outlines key privacy issues in smart home healthcare data collection, which include data sensitivity, ownership, consent management, and the risks associated with data inference and profiling. One major privacy issue is the risk of unauthorized access to personal data, as smart home devices often communicate over wireless networks, making them vulnerable to hacking and eavesdropping. Studies have shown that many IoT devices lack robust security measures, making them easy targets for cyber-attacks (Shah, Bhat, & Khan, 2021). Furthermore, the data collected by these devices is often stored on cloud servers, which can also be susceptible to breaches and unauthorised access (Kumar & Chand, 2020).

Table 2. 1*:* Key Privacy Issues in Smart Home Healthcare Data Collection

Privacy Issue	Implications
Data Sensitivity	Health data is highly sensitive and subject to strict regulations (e.g., HIPAA, GDPR) (Tzanou, 2023). Ensuring compliance while maintaining system functionality is challenging (Anand, 2023; Chenthara, Ahmed, Wang, & Whittaker, 2019).
Data Ownership and Control	Questions arise about data ownership and individual control as information flows between devices, systems, and providers (Psychoula, et al., 2018). This can lead to concerns about personal autonomy and reluctance to adopt technologies (Quach, Thaichon, Martin, Weaven, & Palmatier, 2022; Li, Yigitcanlar, Erol, & Liu, 2021).
Consent Management	Pervasive and often passive data collection makes it difficult to ensure informed consent for all data uses, especially for vulnerable populations (Colnago, et al., 2020).
Data Inference and Profiling	Rich datasets can be used to infer sensitive information beyond what was explicitly collected, raising concerns about unauthorised profiling and potential discrimination (Favaretto, De Clercq, & Elger, 2019).

2.2.2 Security Challenges in Healthcare IoT Devices

Healthcare IoT devices, which are often integrated into SHS and form the backbone of SHHE, often have inherent security vulnerabilities that malicious actors can exploit (Zaman,

Khandaker, Khan, Tariq, & Wong, 2022), exposing them to additional security challenges. These devices collect and transmit sensitive health data that, if compromised, can have severe implications for patient safety and privacy. Security vulnerabilities in healthcare IoT devices can arise from various factors, including weak authentication mechanisms, lack of encryption, and outdated software (Hathaliya & Tanwar, 2020). For instance, many healthcare IoT devices use default passwords that are easy to guess, making them vulnerable to unauthorised access. Additionally, some devices do not encrypt data during transmission, allowing attackers to intercept and read sensitive information. Outdated software can also present security risks, as manufacturers may no longer provide updates and patches to address newly discovered vulnerabilities (Abbas, et al., 2024). Some key threats and vulnerabilities are illustrated in Table 2.2.

Table 2. 2: Threats and Vulnerabilities in IoT-enabled Smart Home Healthcare

Threat/Vulnerability	Security Impact
Device Vulnerabilities	IoT devices often lack robust security due to resource constraints, making them susceptible to malware and unauthorised access (Mishra & Pandya, 2021).
Network Security	Interconnected systems create multiple entry points for attackers, with insecure protocols risking data interception and manipulation (Anantula, Raju, Rani, & Manjula, 2024).
Authentication and Access Control	Diverse ecosystems challenge proper authentication, risking unauthorised access to sensitive data and critical devices (Singh, Juneja, & Kaur, 2022).
Software and Firmware Vulnerabilities	Irregular security updates for IoT devices create long-term risks from known exploits (James & Rabbi, 2023).
Physical Security	Less controlled home environments increase risks of physical tampering or theft of devices (Hammi, Zeadally, Khatoun, & Nebhen, 2022).

2.2.3 Specific Privacy Concerns in Smart Home Healthcare Ecosystems

In SHHE, privacy concerns are amplified due to the sensitive nature of the health data being collected and transmitted. Patients may be particularly concerned about who has access to their health data and how it is being used. Issues such as data ownership, informed consent, and the right to privacy become critical in these settings (Rafique, Khan, Khan, & Ally, 2023). One specific concern is the potential for health data to be shared with third parties without the patient's explicit consent. This can occur through data breaches or through intentional sharing by service providers who collect and analyse the data. Patients need assurance that their health data will be kept confidential and only used for purposes they have consented to (Qadri, Nauman, Zikria, Vasilakos, & Kim, 2020).

Another concern is the possibility of re-identification of anonymised data (Bushwick, 2019). Even when data is anonymised, there is still a risk that individuals can be re-identified through data linkage techniques, where anonymized data is combined with other datasets to reveal the identity of individuals (Kim, Oh, Ryu, & Lee, 2020). Moreover, the deployment of SHHE also raises important regulatory and ethical considerations as illustrated in Table 2.3. While DACP and DMA-ABAC comply with HIPAA and NIST guidelines, their access models introduce policy fragmentation across multiple domains. This limitation is mitigated in the proposed framework through unified privacy-preserving authorisation, which enforces GDPR and HIPAA-compliant access control while allowing fine-grained user-driven consent management.

Table 2. 3: Regulatory and Ethical Considerations in Smart Home Healthcare

Consideration	Implication and Challenges
Regulatory Compliance	Navigating complex healthcare regulations (e.g., GDPR, HIPAA) while maintaining SHS functionality requires careful consideration and robust privacy-preserving architectures (Motti & Berkovsky, 2022).
Ethical Use of Data	Balancing the potential societal benefits of health data analysis with individual privacy rights raises ethical questions about data usage and user consent (Wiertz & Boldt, 2022).
Digital Divide and Accessibility	Smart home healthcare technologies may exacerbate healthcare disparities due to limited access based on cost, technological literacy, or infrastructure availability (Pirzada, Wilde, Doherty, & Harris-Birtill, 2022).
Algorithmic Bias	AI and machine learning algorithms used for health data analysis raise concerns about potential biases leading to unfair or discriminatory outcomes (Agarwal, et al., 2023).

Addressing these privacy and security challenges is crucial for the widespread adoption and success of SHHS. The following sections will explore various approaches and technologies aimed at mitigating these risks and enhancing user privacy in these environments.

2.2.4 Blockchain Technology for Privacy Preservation

Blockchain technology (BCT) has emerged as a promising solution for addressing many of the privacy and security challenges in SHS. Blockchain is a decentralised ledger that records transactions in a secure and immutable manner. Each block in the blockchain contains a cryptographic hash of the previous block, a timestamp, and transaction data, making it tamper-proof and transparent (Maleh, Shojafar, Alazab, & Romdhani, 2020; Egala, Pradhan, Badarla, & Mohanty, 2021). Its decentralised, transparent, and tamper-resistant nature offers unique advantages for protecting sensitive health data while enabling secure data sharing among

various stakeholders (Dwivedi, Srivastava, Dhar, & Singh, 2019) In the context of smart home healthcare, BCT has been employed to provide a secure infrastructure for managing and sharing sensitive health data (Rifi, Agoulmine, Chendeb Taher, & Rachkidi, 2018). Exploring the potential of BCT for privacy preservation in SHHE is essential in this current study.

2.2.4.1 Smart Contracts and Their Role in Privacy Preservation

Smart Contracts (SC) function as a critical component within a comprehensive, privacy-preserving framework for smart home healthcare systems (SHHS), working synergistically with additional privacy-control mechanisms to enforce and automate privacy policies. SCs are implemented on a blockchain platform to handle data access and sharing rules, yet they operate within a larger privacy architecture encompassing data visibility controls, storage specifications, and format management (Ullah, Aslam, & Arjomand, 2020; Wang, Xia, Ren, Yuan, & Miao, 2021). In this approach, SCs enable automated, consent-based access control through a publisher-subscriber model. This model allows smart contracts to enforce predefined privacy scores calculated dynamically based on several key factors, including time-decay (λ), role-based weights (ω_r), and data sensitivity (γ_d), which collectively determine access privileges.

By integrating SCs into a multi-layered privacy framework, the study ensure that privacy preferences are not only enforced automatically but are also adjusted in real-time based on contextual and user-defined privacy requirements (Luu, Chu, Olickel, Saxena, & Hobor, 2016). This layered approach addresses comprehensive privacy concerns in SHHS, unifying privacy and security through a robust, adaptive framework.

An exemplary scheme by (Rifi, Agoulmine, Chendeb Taher, & Rachkidi, 2018) utilised a publisher-subscriber algorithm to enhance data access protocols via smart contracts between data providers and consumers in the eHealth domain, where the sensitivity of medical data necessitates robust privacy measures. The InterPlanetary File System (IPFS) was employed as an off-chain storage solution to manage large data volumes, ensuring that only essential contract information and data references are stored on the blockchain. For each newly generated data instance from a sensor associated with a publisher, the gateway (miner) applies content-based indexing with cryptographic hashing to securely store the data in IPFS.

The resulting IPFS hash, which serves as both an index and a pointer to the data's location, is then broadcast to the blockchain. Upon receiving a notification, a subscriber conducts a frontend lookup using a binary search algorithm on the contract's ordered mapping structure, which contains all whitelisted publishers' addresses for verification. This dual-indexing approach, employing IPFS content addressing for data storage and an ordered address mapping for access control, ensures efficient data retrieval and permission verification. By leveraging cryptographic hashing and distributed storage, this scheme optimises data access and retrieval and also strengthens data privacy and integrity in smart home healthcare systems.

The studies by Lin et al. (2019) and Chen, Tang, Guo, Yang, and Xiang (2022) proposed a blockchain-based mutual authentication system for smart homes, called HomeChain. Their system utilises smart contracts to implement access control policies and manage data-sharing permissions. This research demonstrated that smart contracts can effectively enforce privacy preferences and automate compliance with data protection regulations. Similarly, Zhang et al. (2018) explored a decentralised, blockchain-based access control framework, emphasising the role of smart contracts in validating both static and dynamic access rights. The significance of their approach lies in eliminating single points of failure; however, it may encounter challenges when deployed on resource-constrained IoT devices.

Tan, Shi, Yu, Aloqaily, and Jararweh (2021) present a blockchain-enabled framework for green IoT, integrating attribute-based and blockchain access control to ensure secure device management; however, it may encounter scalability limitations. Similarly, Egala, Pradhan, Badarla, and Mohanty (2021) propose the Fortified-Chain framework for IoMT, which combines blockchain with hybrid computing to provide secure, decentralised data storage and access control. Their approach effectively addresses privacy and latency issues but requires extensive computational resources. Gong et al. (2024) introduce a secure and dynamic access control scheme leveraging blockchain technology, emphasising privacy preservation through attribute-based encryption; however, it may face challenges related to high storage overhead on traditional blockchains.

2.2.4.2 Blockchain-based Access Control and Data Sharing

Blockchain technology offers new possibilities for implementing fine-grained access control and secure data sharing in smart home healthcare systems. Various access control mechanisms based on context-awareness features have been proposed to address issues of authentication

and authorisation in IoT-driven environments (Trnka, Cerny, & Stickney, 2018.), including Blockchain-based access control (Malik & Shah, 2022; Ouaddah, Elkalam, & Ouahman, 2017; Outchakoucht, Hamza, & Leroy, 2017) and development of a medical blockchain ecosystem based on a dynamic consent system (Kim, et al., 2021).

The study by Zheng et al. (2024) presented a comprehensive overview of blockchain-based access control mechanisms and highlighted how blockchain can enable dynamic, user-centric access control policies that adapt to the changing context of smart home environments. The authors also discussed how blockchain can facilitate secure and transparent data sharing among multiple stakeholders while maintaining user privacy.

2.2.4.3 Application of Blockchain in Healthcare Data Security

Blockchain can enhance healthcare data security by providing a secure and transparent way to manage patient data. By storing health data on a blockchain, healthcare providers can ensure that the data is immutable and that all access and modifications are recorded transparently. This can prevent unauthorised access and ensure that patients have control over who accesses their data (Tan, et al., 2021). Smart contracts can further enhance data security by automating access control and consent management. Verma, Kawamoto, Fadlullah, Nishiyama, and Kato (2017) propose a smart contract that can be programmed to grant access to patient data only to authorised healthcare providers and under specific conditions, such as for a particular treatment or a defined period.

However, recent work by Hossein et al. (2021) introduced BCHealth, a blockchain-based privacy-preserving architecture designed for IoT-enabled healthcare systems. Their approach effectively enhances data privacy by implementing a dual-chain structure, which separates access control policies from data transactions to improve efficiency and scalability. However, while BCHealth provides fine-grained access control, it primarily relies on static user-defined policies, which offer limited adaptability to evolving privacy contexts and user preferences. Additionally, it lacks integration with machine learning-driven privacy risk assessment and dynamic consent mechanisms, reducing its ability to proactively address real-time privacy violations. In contrast, the proposed framework extends these capabilities by introducing Multi-Dimensional Dynamic Consent (MDDC) and AI-driven privacy controls, ensuring context-aware privacy enforcement and predictive risk assessment.

Similarly, the DMA-ABAC model proposed by Shahraki et al. (2019) leverages Attribute-Based Group Signature (ABGS) to enable decentralised, cross-domain access control without relying on a central authority. While this approach effectively strengthens secure access control across multiple healthcare domains, it primarily focuses on authentication rather than comprehensive consent management. Moreover, the proposed decentralised multi-authority ABAC mode (DMA-ABAC) reliance on independent attribute authorities introduces management complexities. The model successfully addresses security requirements such as attribute collision resistance and flexible access control; however, it provides limited consideration for temporal dynamics and data sensitivity classifications, which are crucial for context-aware privacy in smart home healthcare environments. Likewise, Salehi et al. (2023) present DACP, integrating attribute-based signatures for secure cross-domain authentication. However, both models provide only limited support for comprehensive consent management mechanisms, thereby restricting user control over data disclosure. In contrast, the proposed framework extends beyond access control by incorporating dynamic consent policies, privacy-preserving encryption, and blockchain-based auditability to enhance security and patient autonomy.

2.2.4.4 Challenges and Opportunities of Using Blockchain for Privacy in Smart Homes

While blockchain technology offers significant potential for enhancing privacy and security, it also presents several challenges. One major challenge is scalability, as the blockchain size can grow rapidly with the addition of new transactions, making storage and management increasingly difficult (Moosavi et al., 2015). Moreover, Yánez, Mahmud, Bahsoon, Zhang, and Buyya (2020) acknowledged the potential benefits of blockchain applications in IoT systems, including smart homes. However, their study identified several challenges, such as scalability issues, high energy consumption, and the need for standardisation. The study emphasised that addressing these challenges is crucial for the effective deployment of blockchain in resource-constrained IoT environments.

Furthermore, Wirth and Kolain (2018) explored the challenges of using blockchain for GDPR-compliant data protection. Their study highlighted potential conflicts between blockchain's immutability and GDPR requirements, such as the right to be forgotten (Barth, 2021). The proposed solutions include the use of off-chain storage and advanced cryptographic techniques. Additionally, while blockchain immutability is a strength in terms of security, it can also be a

limitation, as it does not allow for the deletion or modification of data, which can be problematic in certain scenarios (Alzaabi & Mehmood, 2024).

Moreover, implementing blockchain in SHHE requires significant computational resources and energy, which can be a barrier to adoption. Despite these challenges, the opportunities presented by blockchain for enhancing privacy and security in smart homes are substantial, and ongoing research and development are likely to address many of these issues (Othman, Almalki, Chakraborty, & Sakli, 2022).

Blockchain technology offers a promising avenue for enhancing privacy preservation in SHHS. However, its implementation comes with significant challenges. As the field evolves, researchers and developers must prioritise addressing the current limitations of blockchain-based solutions. Key areas for future work include improving scalability, reducing energy consumption, and ensuring compliance with data protection regulations. The goal should be to develop innovative blockchain-based approaches that strike an optimal balance between robust privacy protection, efficient system performance, and adherence to regulatory requirements. Such advancements will be essential for realising the full potential of BCT within the unique and sensitive context of SHHS.

Despite the numerous benefits the SHHs offer, it also introduces significant privacy and security challenges. Addressing these challenges requires robust security measures, comprehensive privacy policies, and the implementation of advanced technologies like blockchain to ensure the protection of sensitive health data. The following sections will explore existing privacy preservation schemes and their limitations, providing further insight into how these challenges can be addressed.

2.2.5 Ethical Information Disclosure in Smart Home Healthcare

The ethical disclosure of information in SHHE is a critical component of the proposed privacy model. This synthesis aims to establish a framework that balances the need for data sharing in healthcare contexts with the imperative to protect individual privacy rights (Mittelstadt, Allo, Taddeo, Wachter, & Floridi, 2016; Tsamados et al., 2021). Drawing from various ethical principles and contemporary privacy theories, a comprehensive approach to ethical information disclosure is developed.

The development of smart home healthcare systems has fundamentally changed how personal health data is collected, processed, and shared. As aptly observed by Solove and Schwartz (2020), *"Wherever we go, whatever we do, we could easily leave behind a trail of data that is recorded and gathered together. These new technologies, coupled with the increasing use of personal information by businesses and government, pose new challenges for the protection of privacy."* This observation underscores the critical need for a robust methodology that addresses both the technical and ethical dimensions of privacy protection in smart home healthcare environments.

To contextualise the ethical issues in greater depth, the following sections explore the specific ethical principles, user consent dilemmas, and regulatory compliance factors, highlighting both established findings and current gaps identified in the literature.

2.2.5.1 Ethical Principles Guiding Data Disclosure

The ethical handling and disclosure of personal data have become increasingly critical, particularly within smart home healthcare ecosystems. As observed by Solove and Schwartz (2020), pervasive data collection poses significant ethical risks, notably when users remain unaware or uninformed about how their personal information is being processed or shared. To mitigate these risks, researchers advocate for a consent-based ethical framework that places users at the centre of data-handling decisions. Prioritising consent not only aligns with contemporary ethical standards but also significantly enhances transparency, thereby fostering greater trust between users and healthcare technology providers.
Three core ethical principles underpin effective and ethically sound data disclosure:

1. **Transparency:** Users must be fully informed regarding the nature and scope of data collected, the purposes for its use, and the identities of parties with access (Patil, Joshi, & Patil, 2020; Rossi & Lenzini, 2020). Transparency is crucial for enabling users to make informed decisions, clearly communicating the practical implications of data-sharing activities.
2. **User Consent:** Effective ethical disclosure requires robust mechanisms for obtaining and managing informed consent. Users should possess the capacity to freely provide, withhold, or revoke consent concerning their personal data at any stage of data handling (Ploug & Holm, 2020). Consent processes should be intuitive, easily manageable, and adaptable to changing user preferences and circumstances.

3. **Data Minimisation:** Only essential data needed for explicitly stated purposes should be collected and processed, limiting exposure to unnecessary privacy risks (Crutzen, Ygram Peters, & Mondschein, 2019). Adhering strictly to the principle of data minimisation can significantly reduce vulnerabilities and enhance users' trust by demonstrating commitment to responsible and limited data usage.

Together, these ethical principles i.e., transparency, informed consent, and data minimisation, form a robust foundation for ethical data disclosure within smart home healthcare systems. They serve as guiding standards, helping balance the need for valuable data sharing and analysis with the imperative of safeguarding individual privacy rights.

2.2.5.2 Addressing the Consent Dilemma

Managing consent in the digital age, particularly within smart home healthcare ecosystems, is notably complex. This challenge was presciently identified by Branscomb (1994), who highlighted that individuals frequently experience difficulties comprehending or managing privacy-related decisions amidst complex data ecosystems. Solove (2013) further elucidated this as the "Privacy Self-Management and the Consent Dilemma," emphasising the challenges individuals face in making fully informed privacy decisions when interacting with sophisticated digital technologies.

This dilemma arises primarily due to the intricate and pervasive nature of data collection processes within SHHE, where users often lack clarity regarding the exact implications of their privacy choices. To address this, the approach adopted in this research advocates several targeted strategies:

1. **Contextual Privacy Policies:** Rather than burdening users with extensive, complex privacy documents, concise and context-specific privacy information is provided directly at points of data collection or sharing (Khanna & Srivastava, 2020; Alagar, Alsaig, Ormandjiva, & Wan, 2018). This ensures that users clearly understand the privacy implications pertinent to specific situations, facilitating informed decision-making.

2. **Dynamic Consent Management:** To accommodate the dynamic nature of privacy preferences, the proposed privacy framework incorporates mechanisms enabling users to easily grant, modify, or revoke consent dynamically. This flexibility is crucial in

SHHE, where privacy needs and contexts frequently evolve (Abutaleb, Alqahtany, & Syed, 2023; Mamo, Martin, Desira, Ellul, & Ebejer, 2020).

3. **Simplified User Interfaces:** Consent management interfaces are designed to be intuitive and user-friendly, ensuring that users can effectively understand and manage their privacy preferences without experiencing decision fatigue (Crabtree, et al., 2018). This approach leverages agile prototyping and user-centric design methodologies, continuously refining interfaces based on direct user feedback and practical usability assessments.

These strategies collectively help overcome the "Privacy Self-Management and Consent Dilemma" identified by Solove (2013), offering users clearer, contextually relevant choices that effectively balance the benefits of data sharing with privacy protections. By simplifying the consent management process and enhancing user control, the proposed framework promotes greater user autonomy and privacy compliance in smart home healthcare systems.

2.2.5.3 Balancing Benefits and Risks

Ethical disclosure of information within SHHEs requires careful balancing of potential benefits against associated privacy risks. To achieve this balance, an effective ethical disclosure framework should incorporate specific measures that delineate the conditions and limits of data use, minimising potential misuse while maximising healthcare benefits. Key mechanisms proposed for effectively balancing these factors include:

1. **Tiered Access Control:** Implementing role-based access control ensures that sensitive healthcare data is accessible only to those authorised and with legitimate purposes (Zhang, et al., 2021; Wu, Zhang, Gao, & Xie, 2024). Such mechanisms limit unnecessary data exposure, significantly mitigating privacy risks while facilitating necessary access for caregivers, healthcare professionals, and other relevant stakeholders.

2. **Temporal Data Sensitivity:** Recognising that data sensitivity often diminishes over time, incorporating a temporal sensitivity factor or time-decay approach allows for adaptive ethical data retention and sharing policies (Cardoso, 2023; Chen & Huang, 2023; Pu, Jiang, Song, Liang, & Yang, 2024). This approach ensures that data

considered critical in real-time scenarios can be appropriately managed and protected, while less sensitive historical data can be utilised more flexibly, optimising data utility.

3. **User Empowerment and Control:** Providing users with accessible, intuitive interfaces empowers them to manage their data proactively. Clear, context-specific information enhances users' understanding of privacy implications, enabling them to make informed decisions regarding data disclosure (Masmoudi & Saeed, 2024). User-centric tools and mechanisms bolster user confidence and trust, essential for broad adoption of SHHE technologies.

Through these targeted strategies, the framework systematically addresses the critical task of balancing the significant benefits derived from data sharing such as improved healthcare outcomes and personalised care with the imperative of robust privacy protection. This balanced approach addresses ethical considerations effectively and enhances user acceptance and adoption of smart healthcare technologies.

2.2.5.4 Compliance with Regulatory Frameworks

Compliance with regulatory frameworks such as GDPR and HIPAA is essential for ethical data disclosure within SHHEs. The ethical disclosure framework integrates regulatory compliance through structured mechanisms to ensure data handling aligns with stringent privacy and data protection standards:

1. **Auditable Consent Records:** Utilising blockchain technology, all consent-related transactions are recorded immutably. This approach provides clear, auditable records of user consent, supporting regulatory compliance and facilitating transparency (Hang, Kim, Kim, & Kim, 2021; Velmovitsky, Bublitz, Fadrique, & Morita, 2021).

2. **Data Portability:** Aligning with GDPR requirements, the ethical framework supports data portability, enabling users to easily access and transfer their personal data across different service providers. This capability empowers users and complies explicitly with GDPR regulations, thus enhancing user control and trust (Janssen, Cobbe, Norval, & Singh, 2020).

3. **Purpose Limitation:** Clear specification of purposes for data use and strict enforcement through blockchain-enabled smart contracts ensure data processing aligns

strictly with user-approved purposes, adhering to regulatory requirements such as GDPR and HIPAA (Wirth & Kolain, 2018). This strategy mitigates risks associated with data misuse or unauthorized secondary data use.

By incorporating robust blockchain-enabled mechanisms for consent management, data portability, and purpose-specific data handling, this approach systematically addresses key regulatory demands. Thus, it ensures both the ethical integrity and legal compliance necessary for the sustainable and trusted operation of smart home healthcare ecosystems.

2.3 Existing Privacy Preservation Schemes and Their Limitations

Privacy preservation in Smart Home Healthcare Ecosystems (SHHE) is critical due to the sensitive nature of the data involved. As smart home healthcare systems expand, robust privacy-preserving schemes are increasingly necessary to address emerging challenges. The evolution of privacy preservation approaches can be categorised into three generations: traditional methods, modern privacy-enhancing technologies (PETs), and hybrid solutions. Each generation builds upon its predecessor while addressing distinct challenges.

Traditional methods, often considered the first generation, include basic encryption, access control, data anonymisation techniques, and pseudonymisation approaches. These foundational methods provided baseline privacy protection but struggled to adapt to the dynamic and interconnected nature of SHHE. Modern privacy-enhancing technologies, comprising the second generation, introduced techniques such as differential privacy, homomorphic encryption, and secure multi-party computation. While these advanced methods offered stronger privacy guarantees, they often incurred high computational overhead, limiting their scalability and applicability in resource-constrained environments.

The current generation of hybrid solutions integrates multiple privacy-preserving techniques to balance privacy protection with system usability and efficiency. Blockchain-based privacy frameworks, AI-enhanced privacy protection, and context-aware privacy models exemplify this approach. These solutions address unique SHHE challenges, including the secure acquisition, transmission, storage, and access of sensitive healthcare data, while enhancing

adaptability to real-time scenarios. Despite their advancements, gaps remain in these approaches, particularly regarding interoperability, scalability, and user-centric design.

This section examines privacy preservation schemes chronologically, evaluating their implementation methodologies and effectiveness in SHHE contexts while discussing their specific limitations. Through this analysis, the study identifies critical gaps in current approaches that inform the development of more effective privacy-preserving solutions.

2.3.1 Traditional Privacy Models in Healthcare

Traditional privacy models in healthcare primarily focus on data anonymisation and encryption to protect patient information. Anonymisation techniques, such as data masking and pseudonymisation, aim to remove or alter PII to prevent the re-identification of individuals. However, these methods often fall short as sophisticated data linkage techniques can sometimes re-identify anonymised data by correlating it with other datasets (Bushwick, 2019; Hossain, 2016). Considering cryptographic primitives and lightweight cryptography, these techniques form the foundation of many privacy preservation schemes in IoT and smart home environments. Traditional cryptographic methods, however, often prove too resource-intensive for constrained IoT devices.

As a result, lightweight cryptography has emerged as a promising solution. Dhanda, Singh, and Jindal (2020) conducted a comprehensive survey of lightweight cryptography techniques suitable for IoT environments, highlighting the potential of Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) as effective solutions against emerging threats in resource-constrained IoT devices. However, they noted that while ECC offers strong security, it lags in speed due to its memory requirements.

Hybrid encryption, for data at rest and in transit, is another privacy-preservation technique employed for its inherent speed, confidentiality, and integrity benefits. Encryption algorithms such as AES and RSA (Rivest–Shamir–Adleman) or ECC, are widely used in hybrid models to protect data from unauthorised access. While encryption provides a robust layer of security, it does not address all privacy concerns, particularly those related to data access and usage once decrypted (Surya, Ranichandra, & Ranjani, 2018).
Hence, the limitations of cryptographic scheme implementation in SHHE include:

- Resource constraints of IoT devices can limit the implementation of robust cryptographic solutions.
- Key management in distributed IoT environments remains a significant challenge.
- The trade-off between security strength and computational efficiency often leads to compromises in either security or performance.

2.3.2 Modern Privacy Preservation Techniques

Recent advancements in privacy-preserving technologies have introduced more sophisticated methods to protect sensitive data in smart home healthcare environments. These techniques include differential privacy, privacy-preserving transparency, privacy by design (PARROT) (Alhirabi, et al., 2023; Alkhariji, De, Rana, & Perera, 2023), and privacy-enhancing technologies (PETs).

2.3.2.1 Differential Privacy

Differential Privacy (DP) has emerged as a promising approach for privacy-preserving data analysis, offering mathematical privacy guarantees. DP is a technique designed to provide strong privacy guarantees by adding statistical noise to datasets i.e., adds controlled noise to query results, making it difficult to infer individual data points. This approach ensures that the removal or addition of a single data point does not significantly affect the outcome of any analysis, thereby protecting individual privacy.

The study (Jayaraman & Evans, 2019) evaluated the practical implications of differential privacy in machine learning, highlighting both its potential and limitations. The work revealed that while differential privacy can provide strong privacy guarantees, it often comes at the cost of reduced model accuracy, especially for complex learning tasks. Other limitations are:

- The privacy-utility trade-off in differential privacy can be significant, potentially limiting the usefulness of the protected data for certain applications.
- Determining the appropriate privacy budget (ε) remains challenging and often requires domain expertise.
- Implementing differential privacy in distributed IoT environments poses technical challenges, particularly in managing the privacy budget across multiple data sources.

Differential privacy is particularly useful in scenarios where aggregate data analysis is required without exposing individual data points (Bun & Steinke, 2016). However, the challenge lies in

balancing privacy with data utility, as excessive noise can render the data useless for meaningful analysis (Tschantz, Sen, & Datta, 2020; Miranda-Pascual, Guerra-Balboa, Parra-Arnau, Forné, & Strufe, 2023).

2.3.2.2 Privacy-Preserving Transparency

Privacy-preserving transparency focuses on making data processing activities transparent to users while preserving their privacy. This involves informing users about what data is being collected, how it is being used, and who has access to it. Techniques such as consent management and audit trails are employed to ensure that users have control over their data (Bergram, Bezençon, Maingot, Gjerlufsen, & Holzer, 2020). Despite its benefits, achieving true transparency can be complex, especially in IoT environments where multiple devices and stakeholders are involved (Aqeel, et al., 2022). While privacy-preserving transparency focuses on making data processing activities visible to users, current approaches treat consent and transparency as predominantly static, one-dimensional concepts.

Recent blockchain-based healthcare architectures, such as BCHealth (Hossein et al., 2021), introduce effective privacy preservation mechanisms by leveraging blockchain for secure access control. Their framework enhances data confidentiality and access management within IoT-enabled healthcare environments. However, while BCHealth provides a structured access control mechanism, it scarcely incorporates sophisticated multi-dimensional consent management, which is essential in smart home healthcare ecosystems where privacy preferences vary dynamically across different stakeholders and contexts. This highlights the need for more adaptive, fine-grained consent models that dynamically adjust based on real-time user interactions and evolving privacy constraints. Similarly, while PROUD (Belguith et al., 2020) effectively implements attribute-based access control for IoT applications, it does not fully account for the dynamic nature of consent across different data types, temporal contexts, and access scenarios. Furthermore, existing transparency mechanisms often have limitations in addressing how privacy preferences and consent requirements may evolve across these multiple dimensions simultaneously. For instance, while basic consent management systems allow users to grant or deny access to their data i.e. implement binary consent decisions, they typically cannot handle scenarios where a user might want to:

- Grant different levels of access to the same data type based on temporal factors
- Automatically adjust privacy controls based on data sensitivity decay over time

- Manage consent differently for various combinations of data types and user roles
- Implement dynamic privacy controls that adapt to changing healthcare contexts

These limitations in current approaches highlight the need for a more sophisticated, multi-dimensional approach to consent management and privacy preservation in smart home healthcare environments. Such an approach must consider not only the basic aspects of data privacy but also the complex interplay between different dimensions of consent and how they evolve.

2.3.2.3 Access Control Mechanisms

Access control mechanisms play a crucial role in ensuring that only authorised entities can access sensitive data in smart home healthcare systems. Various access control models have been proposed, including Role-Based Access Control (RBAC) (Chen, et al., 2018; Ameer, Benson, & Sandhu, 2022), Attribute-Based Access Control (ABAC) (Tasali, Chowdhury, & Vasserman, 2017; Ameer, Benson, & Sandhu, 2022), and Capability-Based Access Control (CBAC) (Awan, et al., 2019; Gusmeroli, Piccione, & Rotondi, 2013).

Psychoula, Chen, and Amft (2020) explored user perceptions and attitudes toward smart home technologies, highlighting the importance of user-centric access control mechanisms. Their research emphasised the need for flexible and context-aware access control systems that can adapt to the dynamic nature of smart home environments. Furthermore, recent research in attribute-based access control, such as the PROUD system (Belguith et al., 2020), relies heavily on cryptographic approaches with limited consideration for dynamic consent and user-centric design.

The DACP framework by Salehi et al. (2023) attempts to address some of these integration and adaptability challenges by combining traditional ABAC with cryptographic ABGS for cross-domain environments. This hybrid approach enables secure attribute exchange across domains while preserving user privacy. However, while DACP provides dynamic attribute-based authorization, its support for comprehensive consent management mechanisms remains limited, restricting users from expressing fine-grained, context-dependent privacy preferences. Additionally, like many existing approaches, it offers no explicit integration of data sensitivity classifications or machine learning-driven risk assessment, which could further enhance the adaptability of access control decisions in dynamic healthcare environments.

This proposed framework addresses these limitations by incorporating context-aware access control with dynamic privacy scoring. Moreover, significant research gaps exist in current access control approaches, such as;

1. ***Integration***: Existing access control models lack seamless integration between privacy preservation and user accessibility. While RBAC provides structured role-based permissions and ABAC offers flexible attribute-based policies, neither fully addresses the need for dynamic, context-aware privacy protection that maintains user-friendly access.

2. ***Adaptability***: Traditional access control models struggle to adapt to the dynamic and heterogeneous nature of IoT environments found in smart home healthcare, where access needs can vary based on context, time, and user role. This inflexibility limits their effectiveness in environments where access requirements constantly evolve.

3. ***Implementation***: Implementing and managing fine-grained access control policies is challenging in SHHS, given the complex interactions between devices, users, and data sensitivity levels. Existing solutions often lack intuitive interfaces for managing access control policies, increasing the risk of misconfiguration and unauthorised access.

4. ***Context-Awareness***: Existing models fail to adequately consider the temporal and contextual factors that influence access control decisions in healthcare settings, particularly regarding data sensitivity and user roles over time. The lack of user-friendly interfaces for managing these complex contextual policies further compounds the challenge of maintaining effective access control.

These limitations emphasise the need for a more comprehensive approach that combines robust access control with user-centric design and context awareness, particularly in privacy-sensitive smart home healthcare environments.

2.3.2.4 Data Anonymisation and De-identification Techniques

Data anonymisation and de-identification techniques aim to protect individual privacy by removing or obfuscating personally identifiable information. Common approaches include k-anonymity, l-diversity, and t-closeness. However, traditional data anonymisation and de-identification techniques face significant limitations when applied to smart home healthcare systems (SHHS). Studies by Khalid, Qayyum, Bilal, Al-Fuqaha, and Qadir (2023) and

Gkoulalas-Divanis and Loukides (2014) highlight that these methods often struggle to balance privacy protection with data utility, particularly in the context of rich, interconnected IoT data streams. The dynamic and continuous nature of smart home health data further exacerbates these challenges, as conventional approaches are typically designed for static datasets.

Moreover, advanced analytics and inference attacks can potentially circumvent traditional anonymisation efforts, exposing vulnerabilities. The complexity of smart home healthcare data also necessitates context-specific privacy solutions, as generic methods may not adequately address the unique requirements of this domain. These limitations underscore the need for more sophisticated, adaptive privacy preservation techniques tailored to the evolving landscape of smart home healthcare.

2.3.3 Limitations and Challenges of Current Privacy Schemes in IoT-based Smart Healthcare

While existing privacy preservation schemes offer valuable tools and significant benefits for protecting user privacy in SHHE, they face several limitations and challenges when applied to these complex, dynamic environments. These constraints are explored with highlights on the need for more advanced and tailored solutions as follows:

1. Re-identification Risks: Despite anonymisation efforts, there remains a risk of re-identifying individuals through advanced data linkage techniques (Rocher, Hendrickx, & De Montjoye, 2019). This limitation is particularly concerning in healthcare, where sensitive health data can be misused if re-identified (Culnane, Rubinstein, & Teague, 2017; Pham, Tran, & Nakashima, 2018). The effectiveness of anonymisation can be compromised by the richness and interconnectedness of IoT data, enabling re-identification through data correlation.

2. *Inference Attacks and Data Correlation*: Advanced data analytics and machine learning techniques have made it increasingly possible to infer sensitive information from seemingly innocuous data. Chenthara, Ahmed, Wang, and Whittaker (2019) highlighted that traditional anonymisation techniques might be insufficient to prevent such inference attacks, particularly given the rich, multidimensional data generated in SHHSs.

3. Balancing Privacy and Utility: Techniques like differential privacy introduce noise to protect privacy, which can compromise the utility of the data. Striking the right balance between privacy and data utility is a significant challenge (Dwork & Roth, 2014), especially in

healthcare applications where accurate data is crucial for patient care (Dankar & El Emam, 2013; Shahnaz, Qamar, & Khalid, 2019). Moreover, anonymisation techniques often struggle to balance privacy protection with data utility. One of the most significant challenges in privacy preservation is maintaining data utility while ensuring strong privacy guarantees. As pointed out (Al-Sharhan, Omran, & Lari, 2019), techniques like differential privacy often involve a direct trade-off between privacy strength and data usefulness. In healthcare contexts, where data accuracy can be critical for diagnosis and treatment, this trade-off becomes particularly problematic.

4. Complexity of Implementation and *Dynamic Nature*: Implementing advanced privacy-preserving techniques such as differential privacy and privacy-preserving transparency requires significant computational resources and expertise. This complexity can be a barrier to adoption, particularly for smaller healthcare providers and smart home developers (Suriyakumar, Papernot, Goldenberg, & Ghassemi, 2021; Apthorpe, Reisman, & Feamster, 2017). Dynamic and continuous data streams in smart home healthcare pose challenges for traditional anonymisation approaches designed for static datasets. Likewise, the fluid and context-dependent nature of SHHE poses challenges for static privacy models. (Yu, Liu, Pu, Gursoy, & Truex, 2019) emphasised that user privacy preferences may change based on context (e.g., emergencies vs. routine monitoring), time of day, or even health status. Current approaches often lack the flexibility to adapt to these dynamic requirements, potentially leading to overly restrictive or insufficiently protective measures.

5. Regulatory Compliance and Cross Border Data Flows: Ensuring compliance with privacy regulations such as GDPR and HIPAA while maintaining system functionality is essential but remains a significant challenge. Privacy preservation schemes are to be designed to meet regulatory requirements (Bygrave, 2017), which can vary across regions and evolve over time (Zhang & Lin, 2018; Hoofnagle, Van Der Sloot, & Borgesius, 2019). In addition, (Gross & Miller Jr, 2019) pointed out that the global nature of many smart home and healthcare technologies further complicates this issue, as data may flow across jurisdictions with different regulatory requirements.

6. Scalability and Performance Issues: Many privacy-preserving techniques, especially those involving blockchain and differential privacy, face scalability issues. As the volume of data and the number of connected devices grow, maintaining the performance and efficiency of these schemes becomes increasingly difficult (Zyskind & Nathan, 2015; Xiao & Xiong, 2015;

Zheng, Mukkamala, Vatrapu, & Ordieres-Mere, 2018). Furthermore, SHHE systems often involve a large number of heterogeneous devices generating continuous streams of data. Many current privacy preservation techniques struggle to scale effectively in this environment. For instance, (Butun, Sari, & Österberg, 2019) highlighted that traditional encryption methods can introduce significant latency and computational overhead, particularly problematic for resource-constrained IoT devices. This can lead to degraded system performance and potential delays in critical healthcare monitoring and response.

7. *Interoperability and Standardisation*: The lack of standardisation in IoT and smart home technologies creates significant hurdles for implementing consistent privacy measures. As noted in (Torre, Chennamaneni, & Rodriguez, 2023) that the diversity of devices, communication protocols, and data formats in smart home ecosystems makes it challenging to apply uniform privacy preservation techniques across all system components.

8. *User Understanding and Control*: Many current privacy preservation approaches are complex and opaque to end-users. Studies in (Park, Lenhart, Zimmer, & Vitak, 2023; Psychoula, et al., 2018) found that users often struggle to understand and effectively manage their privacy settings in smart home environments. This lack of user-friendly interfaces and comprehensible privacy controls can lead to misconfigurations or hesitancy in adopting these technologies.

9. *Long-term Data Protection*: Smart home healthcare systems often collect and store data over extended periods to track health trends and provide personalised care, and this brings about the issue of secure data retention. Ensuring the long-term protection of this data, especially as encryption standards and privacy technologies evolve, poses a significant challenge. (Yao, et al., 2021) emphasised the need for forward-thinking privacy solutions that can adapt to future technological advancements and emerging threats.

Though it can be said that significant progress has been made in developing privacy preservation schemes for the SHHE, several challenges and limitations remain (Adil, et al., 2024). While the existing privacy preservation approaches offer valuable tools, they face significant limitations when applied to the complex, dynamic, and sensitive environment of smart home healthcare systems (Azad, Arshad, Mahmoud, Salah, & Imran, 2022; Vardalachakis & Tampouratzis, 2024). The dynamic, heterogeneous, and data-rich nature of these environments poses unique challenges that often push the boundaries of traditional

privacy-preserving approaches (Popoola et al., 2024). Addressing these challenges requires innovative solutions that can balance strong privacy protections with system functionality, data utility, user-friendliness, and regulatory compliance that are scalable and easy to implement (Raghav, Choudhary, Pandey, Singh, & Varshney, 2025). Hence, a focus on developing more adaptive, context-aware privacy mechanisms that can effectively navigate the unique challenges of SHHE is essential.

2.4 Context-Aware Privacy Models

Privacy models that incorporate contextual information are essential for managing the dynamic nature of data access and usage in smart home healthcare ecosystems (Sylla, Chalouf, Krief, & Samaké, 2021; Alotaibi & Oracevic, 2023). These models use various contextual factors to adapt privacy controls based on specific circumstances, enhancing the effectiveness and relevance of privacy preservation mechanisms (Diraco, Rescio, Caroppo, Manni, & Leone, 2023). This section explores key elements of context-aware privacy models, including time-decay factors, role-based access control, and sensitivity-based data handling.

2.4.1 Time-Decay Factor in Privacy Models

The concept of the time-decay factor has gained significant attention in the realm of context-aware privacy models. Since the relevance and sensitivity of data tend to diminish over time, incorporating a time-decay function enables privacy models to dynamically adjust the level of data protection (Sylla, Chalouf, Krief, & Samaké, 2021). This approach ensures that older data, which may be less sensitive, is subjected to less stringent privacy controls, thereby achieving a balance between privacy and data utility (Luo et al., 2018).

The primary advantage of incorporating a time-decay factor in privacy models is the ability to balance privacy and data utility. By gradually reducing the protection level of older, less sensitive data, these models enable more flexible data usage without compromising user privacy (Jiang, Wang, & Li, 2020). This approach is particularly relevant in scenarios such as smart home healthcare, where real-time health data is highly sensitive initially but becomes less critical over time (Liu, Ouyang, Liu, & Chen, 2017; Qing, Ibrahim, & Nies, 2024). Moreover, the time-decay factor helps reduce the computational overhead associated with maintaining high levels of privacy protection for all data, regardless of age or relevance (Fang, et al., 2021). By dynamically adjusting the protection level, privacy models can optimise

resource allocation and improve overall system efficiency. For example, in a smart home healthcare setting, real-time health data such as heart rate or blood pressure readings are highly sensitive when first collected but may become less critical over time. By incorporating a time-decay factor, the privacy model can gradually reduce the protection level of this data, allowing for more flexible data usage without compromising user privacy (Jiang, Liu, Zhang, Ding, & Tian, 2024).

However, despite its benefits, the application of the time-decay factor in privacy models faces several limitations and challenges. One key issue is the determination of an appropriate decay function that accurately reflects the diminishing sensitivity of data over time (Chen, et al., 2021). The choice of decay function may vary depending on the specific context and nature of the data, requiring careful consideration and validation. In addition, the time-decay factor may not adequately address the privacy concerns of individuals who place a high value on the long-term protection of their data (Rivadeneira et al., 2023a; Rivadeneira et al., 2023b). In such cases, the gradual reduction of privacy protection may not align with user preferences, leading to potential privacy violations.

To address the limitations and challenges associated with the time-decay factor in privacy models, future research should focus on developing more sophisticated decay functions that consider the diverse privacy preferences of users (Shang, 2017). This could involve incorporating user feedback and allowing for customisable decay rates based on individual privacy requirements. Furthermore, future work should explore the integration of the time-decay factor with other context-aware privacy mechanisms, such as location-based privacy and purpose-based access control (Bhadoria, Saha, Biswas, & Chowdhury, 2021; Patel & Patel, 2023). By combining multiple contextual factors, privacy models can provide more comprehensive and adaptive protection for user data.

The incorporation of the time-decay factor in privacy models offers a promising approach to balance privacy and data utility by dynamically adjusting the level of protection based on the age and relevance of data. While this approach has demonstrated benefits in various scenarios, such as smart home healthcare, it also faces limitations and challenges that require further research and development. By addressing these issues and exploring future directions, privacy models can more effectively protect user privacy while enabling the responsible use of data in context-aware systems.

2.4.2 Role-based access control and its effectiveness

Role-Based Access Control (RBAC) is a widely adopted approach for managing access rights in complex systems, including smart home healthcare environments. By assigning permissions based on user roles, RBAC simplifies access management and enhances security (Tasali, Chowdhury, & Vasserman, 2017; Chen, et al., 2018). RBAC offers several advantages when applied to smart home healthcare systems. By associating access rights with roles rather than individual users, RBAC reduces the complexity of permission management (Parkinson & Khan, 2022).

In a healthcare setting, different roles such as doctors, caregivers, and family members can be assigned specific access levels, ensuring that sensitive data is only accessible to authorised personnel (Morita, Sahu, & Oetomo, 2023; Amiribesheli, Benmansour, & Bouchachia, 2015). This hierarchical approach minimises the risk of data breaches and improves overall system security (Ragothaman, Wang, Rimal, & Lawrence, 2023). Moreover, RBAC enables the implementation of the principle of least privilege, which stipulates that users should have access only to the resources necessary for their specific tasks (Sikder, Petracca, Aksu, Jaeger, & Uluagac, 2021). By adhering to this principle, RBAC helps prevent unauthorised access and mitigates the potential impact of security incidents.

Despite its benefits, traditional RBAC models may not fully address the unique challenges posed by smart home healthcare environments. These environments are often dynamic and decentralised, requiring more flexibility and adaptability in access control mechanisms (Ameer, Benson, & Sandhu, 2022). Traditional RBAC models may struggle to accommodate the rapidly changing roles and permissions in such contexts. Furthermore, RBAC alone may not sufficiently consider contextual factors such as location, time, and specific user activities, which are critical for making dynamic access control decisions in smart home healthcare environments (Sikder, et al., 2022; Khanpara, et al., 2023). These factors can significantly influence access control decisions in smart home healthcare, where the same role may require different permissions depending on the situation (Ghosh, Chandra, Sachidananda, & Elovici, 2019).

To overcome the limitations of traditional RBAC models, researchers have proposed various enhancements that incorporate contextual information. Context-aware RBAC models extend the basic RBAC framework by considering factors such as location, time, and user activities

(Dutta, et al., 2020). For example, a doctor's access rights may be dynamically adjusted based on their presence, while a family member might only have access to general health information within the smart home or the specific healthcare task being performed.

Additionally, attribute-based access control (ABAC) (Ameer, Benson, & Sandhu, 2022) can be integrated with RBAC to provide more fine-grained and flexible access control (Ameer, Benson, & Sandhu, 2022). ABAC allows access decisions to be made based on the attributes of users, resources, and the environment, enabling more granular and adaptable permissions.

Role-Based Access Control is a valuable approach for managing access rights in smart home healthcare systems. By simplifying permission management and enhancing security, RBAC helps protect sensitive healthcare data. However, traditional RBAC models may lack the flexibility and contextual awareness required in dynamic smart home environments. Enhancing RBAC with context-aware capabilities and integrating it with attribute-based access control can provide more granular and adaptable access control mechanisms, improving the overall security and privacy of smart home healthcare systems. There is a need to focus on developing and evaluating these enhanced RBAC models to ensure their effectiveness in real-world scenarios.

2.4.3 Sensitivity-Based Data Handling

Sensitivity-based data handling involves categorising data based on its sensitivity level and applying appropriate privacy controls accordingly. This approach recognises that not all data requires the same level of protection and that privacy measures should be proportional to the potential impact of data disclosure. In SHHE, data sensitivity can vary widely. For example, basic activity data (e.g., steps taken) might be considered less sensitive than detailed medical records or biometric information. By categorising data based on sensitivity, privacy models can apply stricter controls to more sensitive data, such as encryption, access restrictions, and audit trails, while allowing more flexible handling of less sensitive data (Morrison, 2016; Kumar, Braud, Kwon, & Hui, 2020).

Current cross-domain access control frameworks, such as DMA-ABAC (Salehi et al., 2019) and DACP (Salehi et al., 2023), while effective for secure attribute-based access control, offer limited integration of data sensitivity classifications within their authorisation models. These approaches secure the transfer of attributes across domains but do not explicitly differentiate

access control mechanisms based on the varying sensitivity levels of different data types. This limitation underscores the need for our proposed framework, which integrates the Data Sensitivity Factor (DSF) as a core component of privacy-aware access control in smart home healthcare ecosystems.

Implementing sensitivity-based data handling requires a thorough understanding of the data types involved and the potential risks associated with their disclosure. This approach enhances data protection and also improves system performance by avoiding the over-application of resource-intensive privacy measures to less sensitive data (Majeed & Lee, 2020).

Context-aware privacy models that incorporate elements such as time-decay factors, role-based access control, and sensitivity-based data handling offer a robust framework for managing privacy in smart home healthcare ecosystems. These models provide dynamic and adaptable privacy controls that can respond to the varying contexts in which data is used, ensuring both effective privacy preservation and practical data utility. The following sections will delve into the role of user consent and ethical data disclosure, further exploring how these models can be effectively implemented.

2.5 User Consent Frameworks and Ethical Considerations in Literature

The integration of smart home technologies with healthcare services presents unique challenges related to user consent and ethical data disclosure. Ensuring that users are informed, and their consent is obtained for data collection, processing, and sharing is crucial to maintaining trust and protecting privacy. This section explores the importance of informed consent, the ethical implications of data sharing, and mechanisms for ensuring ethical data disclosure.

In addressing these challenges, several regulatory frameworks provide essential guidance. The GDPR launched in 2016 (EUR-Lex, 2016), in articles 5, 6, and 25, has set stringent data privacy standards across Europe, requiring organisations to adhere to seven core principles outlined in Article 5. These principles emphasise lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability in data processing. Adherence to these principles ensures that data processing activities are conducted responsibly and transparently, safeguarding individual privacy. Notable among other articles is the requirement of consent of the data subject and a legal basis

guiding the procession of personal data by any party (Art.6) and the principle of Data Protection (Privacy) by Design and by Default (Art.25).

Similarly, the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) (OPC, 2019), governs personal information handling in Canada's private sector through ten fair information principles. These principles emphasise accountability, purpose specification, consent, limitation of collection, use, disclosure, and retention, as well as accuracy, safeguards, openness, individual access, and the ability to challenge compliance. Together, these regulations highlight the importance of obtaining explicit consent and implementing stringent measures to protect personal data, thereby reinforcing ethical data disclosure practices.

In the United States, the HIPAA (Edemekong, Annamaraju, & Haydel, 2018; ASPE, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 1996) serves as a critical regulatory framework for protecting personal health information (PHI). HIPAA mandates that healthcare providers, insurers, and other entities involved in handling PHI implement robust safeguards to ensure the confidentiality, integrity, and availability of health data. This includes obtaining explicit patient consent for the use and disclosure of their health information, especially in cases where the data might be shared for purposes beyond direct medical care, such as in research or with third-party service providers. HIPAA also enforces strict limitations on the use and disclosure of PHI, ensuring that any shared information is minimised to what is necessary for the intended purpose.

Complementing HIPAA's focus on healthcare data, the California Consumer Privacy Act (CCPA) (OAG, 2018) extends privacy rights and consumer protections to all residents of California, addressing broader categories of personal information beyond health data. Effective on January 1, 2020, the CCPA empowers California consumers to demand access to the personal information that companies hold about them and imposes restrictions on collecting and selling this data. The CCPA enhances consumer control over personal data, allowing individuals to opt out of the sale of their information and request the deletion of their data, thereby providing a more comprehensive approach to privacy protection across different types of personal information. Together, HIPAA and the CCPA illustrate the multifaceted approach to data privacy in the U.S., where sector-specific regulations like HIPAA are complemented by broader consumer protection laws such as the CCPA. This layered regulatory environment

underscores the importance of robust data protection practices catering to individuals' diverse needs and rights concerning their personal information.

Collectively, GDPR, PIPEDA, HIPAA, and CCPA establish a comprehensive framework for ensuring that user consent is respected and that data is disclosed ethically and securely. By aligning smart home technologies with these global standards and regulations for privacy and data protection, including the GDPR's broad scope, PIPEDA's focus on fair information practices, HIPAA's stringent requirements for health data, and CCPA's enhanced consumer rights in California, healthcare-related applications can better protect user trust and privacy. This alignment ensures that data processing activities are conducted responsibly, respecting the diverse legal landscapes governing personal information. (***Appendix A***: Outline the core principles of the GDPR, the fair information principles of PIPEDA, the robust safeguards required by HIPAA, and the Consumer Rights under CCPA.)

2.5.1 Importance of User Control and Consent in Privacy Management

User control and informed consent are fundamental principles in privacy management, particularly in sensitive domains like healthcare. (Psychoula, et al., 2018) conducted a study on users' privacy concerns in IoT-based applications, emphasising the critical role of user control in fostering trust and acceptance of smart home technologies. The findings highlight that users are more likely to adopt and engage with SHHS systems when they are in control of their data.

Moreover, (Rhee, Ma, Seo, & Cha, 2022; Rock, Tajudeen, & Chung, 2024) investigated users' perceptions and attitudes toward IoT-based smart home technologies including wearables and environmental sensors, revealing that privacy concerns often stem from a lack of understanding and control over data collection and usage. The authors argue that empowering users with granular control over their data can significantly mitigate privacy concerns and enhance the adoption of smart home healthcare solutions.

2.5.2 Privacy-Preserving Architectures and Frameworks

To address the need for user-centric privacy management, researchers have proposed various architectures and frameworks that prioritize user control and consent. (Psychoula, Chen, Yao, & Ning, 2019) introduced a privacy-aware architecture for IoT-enabled systems that

incorporates user preferences and context-aware privacy policies. This approach allows users to define fine-grained privacy rules and provides mechanisms for dynamic policy enforcement based on changing contexts.

Another notable contribution is in studies by (Jo, Ma, & Cha, 2021; Psychoula, Chen, & Amft, 2020), who proposed an integrated holistic model for eHealth systems. Their model emphasises the importance of user-centric design in privacy management, incorporating features such as personalised privacy dashboards and consent management tools. The authors argue that such user-friendly interfaces are crucial for enabling individuals to make informed decisions about their health data privacy.

2.5.3 Privacy Risk Assessment and Mitigation Strategies

Effective user-centric privacy management requires tools that help users understand and mitigate privacy risks. (Rivadeneira, Silva, Colomo-Palacios, & Rodrigues, 2023; Chhetri & Genaro Motti, 2022) explored privacy risk awareness in wearables and IoT devices, proposing a framework for assessing and communicating privacy risks to users. The study's approach aims to enhance users' understanding of potential privacy threats and empower them to make informed decisions about data sharing. Building on this concept, (Shahlaei & Hashemi, 2024; Xiao, Ye, Kanwal, Newe, & Lee, 2022) developed a privacy risk-aware approach to data sharing in smart environments. The method incorporates user preferences and contextual factors to calculate a sensitivity metric for different types of data. This approach enables dynamic, user-centric privacy protection that adapts to individual risk tolerances and preferences.

User-centric privacy management in smart home healthcare presents several ongoing challenges. These include designing intuitive interfaces for complex privacy settings, balancing usability with fine-grained control, and adapting to diverse user needs and preferences. There is a need to focus on developing more sophisticated, adaptive privacy management tools that can learn from user behaviors and preferences over time, providing personalised privacy protection while minimising user burden.

2.5.4 The Role of Informed Consent in Privacy Models

Informed consent is a fundamental principle in privacy models, especially in the context of healthcare (Burkhardt, Boy, Doneddu, & Hajli, 2023; Muravyeva, Janssen, Specht, & Custers,

2020). It involves providing users with clear and comprehensive information about what data is being collected, how it will be used, and who will have access to it (Wachter & Mittelstadt, 2019). Users must also be allowed to agree to or decline these terms before any data collection begins. The process of obtaining informed consent is crucial for respecting user autonomy and ensuring transparency in data practices (Wickramasinghe & Reinhardt, 2021; Wickramasinghe, 2022).

In the SHHE, obtaining informed consent can be complex due to the continuous and often passive nature of data collection. This complex and personal nature necessitates a user-centric approach to privacy management which puts users at the center of privacy decisions while examining various strategies and technologies that empower individuals to control their health data effectively. Devices such as health monitors and environmental sensors collect data round-the-clock, making it challenging to continuously inform and obtain consent from users (Shrivastava & Srikanth, 2023). However, implementing user-friendly consent management interfaces and periodic consent reaffirmation can help address this challenge (Williamson & Prybutok, 2024).

While recent blockchain-based healthcare architectures, such as those proposed by Belguith et al. (2020) and Hossein et al. (2021), have made notable advancements in privacy-preserving mechanisms, their approaches to informed consent remain primarily static and constrained in adaptability. BCHealth (Hossein et al., 2021) effectively enhances data security and access control in IoT-enabled healthcare systems, yet it primarily relies on predefined, static access policies, which do not dynamically adjust to evolving user preferences, stakeholder roles, or contextual privacy changes. Similarly, PROUD (Belguith et al., 2020) employs Attribute-Based SignCryption (ABSC) to strengthen access control mechanisms and policy updates, ensuring data confidentiality and policy flexibility. However, while PROUD allows access policies to be modified without requiring data re-encryption, it does not fully address how privacy preferences evolve across different temporal contexts, sensitivity levels, or multi-stakeholder environments.

Similarly, recent works by Zhang et al. (2023) and Anderson et al. (2023) propose blockchain-enabled privacy frameworks but rely on simplified consent mechanisms that overlook the temporal dynamics of privacy preferences. These existing approaches implement basic consent

management through blockchain and attribute-based access control but lack crucial capabilities to handle multiple dimensions of privacy preferences simultaneously. Given the complexity of smart home healthcare ecosystems (SHHE), where privacy preferences are highly dynamic and consent requirements vary across multiple dimensions, a more adaptive and fine-grained consent framework is necessary to facilitate real-time privacy adjustments, user autonomy, and regulatory compliance.

The consent framework proposed by Qu et al. (2025), while introducing dynamic access control, still cannot effectively manage scenarios where patients need to grant temporary elevated access during emergencies while maintaining privacy preferences for routine care, or where different privacy levels are required for the same data type across different timeframes and stakeholders. The study offers on-chain verification mechanisms, right-to-be-informed compliance, and secure off-chain storage, addressing scalability and transparency concerns. However, its consent management model lacks adaptability to real-time, multi-user healthcare environments, limiting its usability in emergency response scenarios. While these architectures provide foundational privacy preservation mechanisms, their inability to address the dynamic, multi-dimensional nature of consent in healthcare settings highlights the critical need for a comprehensive Multi-Dimensional Dynamic Consent (MDDC) model. Unlike static consent models, the MDDC approach proposed in this work ensures adaptive consent policies, fine-grained access control, and enhanced privacy-preserving cryptographic techniques that cater to real-time healthcare data exchange while maintaining data ownership, patient autonomy, and compliance with informed consent principles.

2.5.5 Ethical Implications of Data Sharing in Smart Healthcare

The ethical implications of data sharing in smart healthcare are significant, as they involve balancing the benefits of data use with the need to protect individual privacy (Yuvaraj, Praghash, & Karthikeyan, 2022). Data sharing can enhance healthcare outcomes by enabling better diagnosis, treatment, and monitoring. However, it also poses risks if the data is misused or falls into the wrong hands (Felber, Tian, Pageau, Elger, & Wangmo, 2023).

One major ethical concern is the potential for discrimination based on health data. If sensitive health information is shared with employers, insurers, or other third parties without proper safeguards, it could lead to discrimination against individuals based on their health status

(Gerke, Minssen, & Cohen, 2020). Ensuring that data-sharing practices are governed by strict ethical standards and regulations is essential to prevent such outcomes (Rahman, Hasan, Rahman, & Momotaj, 2024).

Additionally, there is the issue of data ownership and control. Patients should have ownership of their health data and control over who can access and use it (Chiruvella & Guddati, 2021). This includes the right to withdraw consent and request the deletion of their data. Ethical data disclosure practices must prioritise user control and provide mechanisms for users to manage their data preferences easily (Silva & Soto, 2022).

2.5.6 Mechanisms for Ensuring Ethical Data Disclosure

Implementing mechanisms for ethical data disclosure involves several strategies, including consent management, data minimisation, and transparency (Vourganas, Attar, & Michala, 2022).

1. Consent Management: Effective consent management systems allow users to easily give, manage, and withdraw their consent (Shrivastava & Srikanth, 2023). These systems should provide clear information on data practices and allow users to set their preferences. For example, users can choose to share only specific types of data or limit data sharing to certain parties (Zavalyshyn, Legay, Rath, & Rivière, 2022).

2. Data Minimisation: Data minimisation is the practice of collecting only the data that is necessary for a specific purpose and retaining it only for as long as needed (Yusupova & Ismailov, 2023). This principle helps reduce the risks associated with data breaches and misuse. By limiting the amount of data collected and stored, smart home healthcare systems can enhance user privacy (Adeniyi, Arowoogun, Okolo, Chidi, & Babawarun, 2024).

3. Transparency: Transparency in data practices is essential for building trust with users (Sharma, Chen, & Sheth, 2018). Organisations should provide clear and accessible information about their data policies, including what data is collected, how it is used, and who has access to it. Regular audits and reports on data practices can also help maintain transparency and accountability (Wickramasinghe, 2022).

While existing mechanisms for ethical data disclosure have established foundational approaches to consent management, current solutions exhibit limitations in adapting to the multi-dimensional nature of privacy preferences in healthcare settings. For instance, Hossein et al. (2021) propose BCHealth, a blockchain-based privacy-preserving framework that enhances data security and access control. However, privacy preferences in BCHealth are treated as static parameters, limiting its ability to adjust to evolving user requirements and contextual changes dynamically. Similarly, Belguith et al. (2020) introduce PROUD, a cryptographic framework leveraging Attribute-Based SignCryption (ABSC) for secure access control. While PROUD effectively ensures data confidentiality and supports access policy updates, it does not fully address how privacy preferences evolve over time or how data sensitivity levels impact consent requirements in dynamic healthcare environments.

Moreover, Albalwy et al. (2021) present ConsentChain, a blockchain-based dynamic consent architecture for genomic data sharing, which strengthens transparency and traceability. However, ConsentChain primarily operates on a binary consent model, offering limited flexibility in handling complex scenarios where privacy requirements vary simultaneously across multiple dimensions, such as data type, time sensitivity, and stakeholder roles.
These limitations underscore the need for a more adaptive privacy framework that can dynamically adjust access control policies in real-time, ensuring context-aware, fine-grained, and multi-dimensional privacy enforcement in smart home healthcare ecosystems.

The purpose-based consent model proposed by Tith et al. (2020), although implementing blockchain-based access control for electronic health records, still cannot effectively manage the complex interplay between different privacy dimensions or adapt to changing healthcare contexts. These limitations in current approaches underscore the urgent need for more advanced consent management systems that can handle multiple dimensions of privacy preferences simultaneously while adapting to the dynamic nature of healthcare delivery in smart home environments.

As SHHS continues to evolve, user-centric privacy management will play an increasingly crucial role in its success and adoption. By empowering users with greater control over their health data, these systems can foster trust, enhance privacy protection, and ultimately improve the quality of care delivered in smart home environments. Ensuring user consent and ethical data disclosure in SHHS is critical for protecting privacy and maintaining trust. By

implementing robust consent management systems, adhering to ethical data practices, and maintaining transparency, organisations can address the challenges associated with data collection and sharing. The following sections will explore the identification of gaps in current technologies and methodologies, further highlighting areas for improvement and innovation in this field.

2.6 Conceptual Framework for Ethical and Context-Aware Privacy

The conceptual framework for this privacy model is grounded in Acquisti, Taylor, and Wagman's (2016) foundational insight that *"Privacy is not the opposite of sharing—rather, it is control over sharing."* This understanding frame privacy management as an issue of user control rather than restriction, empowering individuals to make informed and contextually appropriate decisions regarding their personal data.

This conceptualisation aligns closely with the ethical principles previously discussed such as transparency, informed consent, and data minimisation (see Section 2.2.5), and addresses critical challenges associated with managing consent dynamically, particularly highlighted in the "Privacy Self-Management and Consent Dilemma" (Section 2.2.5.2). By embedding these ethical principles within a user-centric, context-aware privacy framework, this conceptual approach effectively addresses the identified gaps in existing IoT and healthcare privacy models, particularly the limited adaptability and insufficient user empowerment (Section 2.4).

The conceptual framework proposed here integrates three key context-aware privacy factors to dynamically adapt privacy preferences:

- **Time-Decay Factor**: Adjusts privacy protections dynamically based on data sensitivity, recognising that the relevance and sensitivity of health data often diminish over time.
- **Role-Based Weighting**: Implements dynamic access control that assigns varied data access privileges according to user roles, ensuring that sensitive data is appropriately accessed based on clear role definitions.
- **Data Sensitivity Classification:** Utilises dynamic sensitivity assessments to classify data according to its potential impact if disclosed, further refining privacy management practices.

These factors collectively enhance privacy scores within the proposed blockchain-based authorisation framework, leveraging smart contracts for automated privacy enforcement, transparency, and auditability (as discussed in Section 2.2.4).

Additionally, by incorporating empirical findings from user surveys regarding their privacy preferences, the proposed framework ensures practical relevance and user acceptance. This approach not only addresses technical and regulatory considerations but also aligns strongly with user perceptions, thereby promoting a balanced and ethical approach to privacy management in smart home healthcare ecosystems.

2.7 AI and Machine Learning Approaches for Privacy and Security

As the SHHS becomes increasingly sophisticated, artificial intelligence and machine learning are playing pivotal roles in enhancing both the functionality and security of these environments. Several studies have emerged to explore how AI and ML technologies are being leveraged to address privacy and security challenges in smart home healthcare (Islam, et al., 2024).

2.7.1 AI-based Anomaly Detection and Threat Intelligence

One of the primary applications of AI in smart home security is anomaly detection. AI algorithms can analyse patterns in device behavior, network traffic, and user activities to identify potential security threats. While traditional Cyber Threat Intelligence (CTI) has been largely explored in cybersecurity, its principles can also be leveraged in privacy-preserving AI frameworks (Rahmati, 2025). In smart home healthcare ecosystems, real-time threat intelligence provides valuable insights into potential data privacy risks, allowing AI models to proactively adapt privacy-preserving mechanisms (Arefin & Simcox, 2024). The reliance on static rule-based privacy scoring mechanisms, as highlighted in Chapter 7, limits adaptability to evolving data access patterns. Integrating CTI into machine learning-based privacy optimisation enhances dynamic privacy risk assessment, enabling intelligent, adaptive privacy preservation strategies (El-Gendy, Elsayed, Jurcut & Azer, 2023). A relatable instance is observed in the work done by (Rehan, 2024; Gudala, Shaik, Venkataramanan, & Sadhu, 2019) which proposed an AI-driven framework for detecting and mitigating security threats in IoT environments. This approach uses machine learning algorithms to establish baseline behavior for devices and users, enabling the system to flag unusual activities that may indicate a security

breach. The authors demonstrated that this method could effectively detect various types of attacks, including DDoS and man-in-the-middle attacks, with high accuracy.

Another example of an AI-driven threat intelligence framework is AI4SAFE-IoT, proposed by HaddadPajouh, Khayami, Dehghantanha, Choo, and Parizi (2020). This system utilises a cyber kill chain model comprising a three-layered AI engine, with each layer interacting with the edge based on a security-as-a-service framework. By implementing cyber threat attribution, hunting, and intelligence, and an intelligent web application firewall, the model detects, attributes, and identifies stages of the attack lifecycle, effectively addressing new or updated versions of existing threats through functional interoperability. Despite achieving an 84.7% success rate compared to peer techniques, the model's primary focus was on the edge layer, and its evaluation metrics were thematic. While AI4SAFE-IoT demonstrated the ability to detect various forms of interception threats, particularly within the perception (sensing) layer of smart home devices, privacy concerns extend across the entire ecosystem of devices, communication, and services in smart homes.

Furthermore, CTI can be leveraged for privacy-preserving AI optimisation. Although CTI has been traditionally associated with security, it presents an untapped opportunity for enhancing privacy preservation in AI-driven systems. By harnessing threat intelligence data, machine learning models can proactively adjust privacy scoring mechanisms, mitigating privacy risks in real time rather than relying solely on static privacy policies. This approach directly addresses the limitations of traditional privacy-preserving frameworks, which lack predictive capabilities and require manual tuning of privacy-utility trade-offs. The ability to detect evolving privacy risks using intelligence-driven AI is essential for building adaptive, scalable privacy-preserving systems in healthcare IoT (Adekunle, et al., 2024).

Understanding users' privacy concerns and preferences in developing mechanisms for enhanced privacy control in smart home healthcare was explored by Psychoula et al. (2018) and Psychoula (2020). The study examined anonymisation and data sharing within Ambient Assisted Living (AAL) and proposed methods to enable privacy-preserving machine learning using differential privacy, specifically, a privacy-preserving deep learning mechanism offering flexible anonymisation and data-sharing capabilities. The proposed method was evaluated using various real and synthetic datasets.

The solution combined IoT technologies and machine learning to provide context-aware and personalised services, demonstrating the feasibility of designing an efficient privacy-preserving machine learning system with negligible costs to utility and performance. Furthermore, the study provides valuable insights for service providers and developers in designing practical, end-to-end privacy-preserving architectures in emerging areas such as privacy-preserving machine learning (ML) and IoT. However, while the approach to data sharing within the framework of differential privacy and the application areas mentioned is exemplary, it offers only passive control over user data privacy.

Building on this concept, Bouij & Berja (2024), Aldaheri, Alwahedi, Ferrag, & Batah (2024) explored the use of deep learning techniques for enhancing threat intelligence in smart home environments. Their work demonstrated that deep neural networks could be trained to recognize cyber-attack patterns and predict emerging security and privacy risks. This further reinforces the importance of integrating CTI-driven insights into privacy-preserving AI frameworks, ensuring continuous adaptation to evolving threats while maintaining optimal privacy-utility trade-offs (Achuthan, Ramanathan, Srinivas, & Raman, 2024).

2.7.2 Privacy-Preserving Machine Learning Techniques

While ML can enhance security, it also raises privacy concerns, particularly when dealing with sensitive health data. To address this, researchers have been developing privacy-preserving machine learning techniques. (Psychoula, et al., 2018) introduced a deep-learning approach for privacy preservation in assisted living environments. The method uses autoencoders to create privacy-preserving representations of sensor data, allowing for useful analytics while protecting individual privacy. This study demonstrated an approach that could maintain high accuracy in activity recognition tasks while significantly reducing the risk of privacy breaches. Another significant contribution in this area comes from (Husnoo, Anwar, Chakrabortty, Doss, & Ryan, 2021; Jarin & Eshete, 2022; Jayaraman & Evans, 2019), who evaluated the practical implications of differential privacy in machine learning. Their work highlighted the trade-offs between privacy guarantees and model utility, providing insights into how these techniques can be effectively applied in healthcare contexts.

Ranjan and Kumar (2024) propose a multi-layer encryption approach that combines deep learning-based encryption with blockchain technology to secure IoT medical data. The study utilises smart contracts within the blockchain to manage access controls and enforce data

integrity during transmission, addressing privacy concerns by employing a dual symmetric encryption scheme (AES + Blowfish) along with optimal key selection through deep learning models (LSTM and CNN). The significance of this study lies in its comprehensive approach to enhancing data security and privacy. However, while the layered encryption model provides additional security, it does not constitute a true hybrid encryption system, which typically integrates both symmetric and asymmetric cryptographic techniques. Additionally, the proposed framework may face computational overhead and real-time implementation challenges due to the complexity of the encryption and key generation techniques.

Furthermore, while Hossein et al. (2021) propose a privacy-preserving framework for blockchain-based healthcare architectures, their model primarily focuses on access control and data security without incorporating machine learning-driven privacy risk assessment capabilities. Although their approach effectively enhances secure data transactions and consent management, it does not leverage AI-driven analytics to predict privacy violations or dynamically adjust privacy policies based on emerging risks. This study addresses this gap by integrating blockchain security with AI-powered privacy enhancements, enabling more sophisticated, adaptive, and risk-aware privacy controls through real-time anomaly detection and dynamic privacy scoring.

2.7.3 Federated Learning and Secure Multi-Party Computation

Federated Learning (FL) has emerged as a promising approach for training machine learning models on distributed datasets without compromising privacy. This is particularly relevant in smart home healthcare, where data is collected across multiple households or devices. Ali, Naeem, Tariq, and Kaddoum (2022) explore how FL addresses privacy concerns in smart healthcare systems, particularly with Internet of Medical Things (IoMT) devices. FL enables distributed AI training without directly accessing confidential patient data, enhancing privacy by sharing only model gradients.

The study reviews privacy issues in IoMT and examines the role of FL in mitigating these risks, emphasising advanced architectures such as deep reinforcement learning, digital twins, and generative adversarial networks to detect privacy threats. While FL offers promising solutions for privacy preservation, challenges such as communication overhead and model accuracy remain, necessitating further research to optimise these systems for real-world applications.

Complementing federated learning, secure multi-party computation (SMPC) techniques offer ways to perform computations on sensitive data from multiple parties without revealing the individual inputs. Cabrero-Holgueras and Pastrana (2021) and Soykan et al. (2022) explored the application of SMPC in smart home healthcare, demonstrating how it can enable secure data analysis across multiple households or healthcare providers.

While AI and ML offer powerful tools for enhancing privacy and security in smart home healthcare, they also introduce new challenges. These include techniques and explainable AI to ensure transparency in decision-making, managing the computational overhead of privacy-preserving techniques, and addressing potential biases in AI algorithms. As the field continues to evolve, future research should focus on developing more efficient and robust privacy-preserving ML techniques, improving the interpretability of AI-driven security systems, and exploring novel applications of AI for privacy enhancement in smart home healthcare environments. By addressing these challenges, AI and ML can play a crucial role in creating secure, privacy-preserving smart home healthcare systems that users can trust and rely on.

2.8 Identification of Gaps in Current Technologies and Methodologies

The rapid evolution of smart home healthcare technologies has brought about significant advancements; however, several gaps and limitations persist in existing technologies and methodologies (Renukappa, Mudiyi, Suresh, Abdalla, & Subbarao, 2022). These gaps are evident in both the technical aspects of privacy models (i.e., the theoretical foundations, algorithms, and designed frameworks) and the practical implementation of privacy-preserving mechanisms. Addressing these shortcomings is essential for the development of robust privacy frameworks in smart home healthcare environments.

2.8.1 Technical and Implementation Gaps

Several technical challenges hinder the effectiveness of privacy models in managing the growing complexity and scale of smart home healthcare systems. For instance, blockchain-based frameworks, while effective for general cybersecurity, often fail to address specific privacy preservation needs in healthcare, such as data sensitivity and contextual consent management (Taylor et al., 2020).

Scalability remains a critical issue as privacy-preserving techniques like differential privacy and homomorphic encryption face difficulties in handling large-scale, real-time data streams (Iqbal, et al., 2021). Additionally, the interoperability of heterogeneous devices is limited due to inconsistent privacy protocols, leading to fragmented privacy protections across smart home ecosystems (Karunarathne, Saxena, & Khan, 2021; Egala, Pradhan, Badarla, & Mohanty, 2021). Computational overhead further exacerbates these challenges, as resource-intensive methods such as secure multi-party computation and advanced encryption exceed the capabilities of many IoT devices (Ma, Naas, Sigg, & Lyu, 2022; Nasir, et al., 2022). While technical limitations pose significant challenges, the gaps in implementing privacy-preserving mechanisms are equally important.

The implementation of privacy-preserving mechanisms is fraught with challenges. Many existing solutions are developed from a technical perspective, often neglecting user-centric design principles and ethical considerations (Akil, Islami, Fischer-Hübner, Martucci, & Zuccato, 2020; El Majdoubi, El Bakkali, Sadki, Maqour, & Leghmid, 2022). This frequently results in privacy models that are difficult for users to understand or manage, thereby reducing their effectiveness (Mehta, Gooch, Bandara, Price, & Nuseibeh, 2021; Wickramasinghe & Reinhardt, 2021).

Moreover, ethical issues such as data ownership, fairness, and consent are inadequately integrated into current models, limiting their capacity to address broader societal concerns (Hummel, Braun, & Dabrock, 2021; Rubeis, 2022; Anom, 2020). Additionally, many proposed privacy-preserving techniques are validated in controlled environments using synthetic data, which fails to capture the complexities of real-world conditions (Mosquera-Lopez et al., 2020). Consequently, these models often lack the robustness needed to perform effectively in diverse healthcare settings (Silva, Gonçalves, Antunes, Curado, & Walek, 2022).

These identified gaps inform the development of this study's methodology, which aims to address both technical and implementation challenges through a comprehensive, user-centric approach.

2.8.2 Opportunities for Enhancements

The challenges in existing frameworks also present opportunities for innovation. Scalable privacy-preserving techniques, such as lightweight cryptographic methods and federated learning models, offer promising avenues for managing large-scale healthcare data while preserving privacy (Irshad, et al., 2023; Altherwi, et al., 2024). Interoperability can be improved by establishing standardised privacy protocols and ensuring consistent protection across devices from different manufacturers (Yusupova & Ismailov, 2023). Ethical considerations, such as balancing consequentialist and deontological principles, should guide the design of privacy frameworks to foster user trust and acceptance (Rahanu, Georgiadou, Siakas, Ross, & Berki, 2021; Pirzada, Wilde, Doherty, & Harris-Birtill, 2022).

Additionally, frameworks that balance technical solutions with ethical principles will foster greater user trust and acceptance (Pirzada, Wilde, Doherty, & Harris-Birtill, 2022; Wirth & Kolain, 2018). While recent blockchain-based healthcare architectures, such as Hossein et al. (2021), provide a solid foundation for privacy preservation and access control, they do not fully incorporate dynamic privacy mechanisms or comprehensive consent management. Their approach remains largely rule-based, limiting its ability to adapt to evolving user preferences, contextual privacy needs, and real-time data sensitivity levels.
This study advances beyond these limitations by integrating Smart contract anomaly detection and dynamic privacy-utility trade-off protocols, enabling more context-aware, adaptive, and risk-sensitive privacy solutions.

Recent access control architectures like DMA-ABAC (Salehi et al., 2019) and DACP (Salehi et al., 2023) demonstrate the potential of decentralised attribute-based approaches for cross-domain healthcare environments. While these approaches effectively address security requirements through cryptographic primitives like Attribute-Based Group Signature (ABGS), they remain largely rule-based, limiting their ability to adapt to evolving user preferences, contextual privacy needs, and real-time data sensitivity levels. This study advances beyond these limitations by integrating blockchain-based smart contract anomaly detection and dynamic privacy-utility trade-off protocols, enabling more context-aware, adaptive, and risk-sensitive privacy solutions.

Participatory design methods, which actively involve users in the development process, can address usability concerns by ensuring privacy mechanisms align with user needs and

expectations (El Majdoubi, El Bakkali, Sadki, Maqour, & Leghmid, 2022; Rovolis & Habibipour, 2024). Empowering users with customisable privacy settings enhances transparency and allows for informed decision-making, fostering trust in smart home healthcare systems. Comprehensive evaluation frameworks that test privacy models in real-world settings are essential to validate their practicality and effectiveness under diverse conditions (Aun, et al., 2024). Moreover, interdisciplinary collaboration among researchers, industry leaders, and ethicists is critical for developing privacy-preserving solutions that are both technically sound and ethically robust.

2.8.3 Proposed Framework

Building on these insights, the proposed framework integrates blockchain, AI, and user-centric strategies to address existing gaps and enhance privacy preservation in smart home healthcare systems, as summarised in Table 2.4. The framework prioritises user consent management, dynamic privacy scoring, and smart contract enforcement to achieve a comprehensive and adaptive privacy solution (Rahman, Hasan, Rahman, & Momotaj, 2024; Shrivastava & Srikanth, 2023). The consent-centric privacy model places user preferences at the forefront of data collection and processing activities, ensuring explicit control over sensitive information (Kim, et al., 2021; Peng, 2022; Zhang, Shanmugam, & Allen, 2023).

Dynamic privacy scoring mechanisms account for factors such as data aging, user roles, and data sensitivity to tailor privacy settings in real-time (Patel & Jadhav, 2024; Hommel & Frings, 2020; Liu, Zhang, Wan, Ji, & Tian, 2020). Additionally, mechanisms are embedded within the system to ensure that users are fully informed about the implications of their consent choices, enhancing transparency and fostering trust in the data management process (Kounoudes & Kapitsaki, 2020).

Unlike existing cross-domain approaches such as DMA-ABAC and DACP that primarily focus on secure attribute exchange and verification, this current study's framework places user consent at the forefront through Multi-Dimensional Dynamic Consent (MDDC). While these previous systems enable secure cross-domain access control, they provide only limited integration of temporal, role-based, and sensitivity factors. In contracts, the proposed model incorporates these elements within a smart contract-based access control scheme to enhance trust and stakeholder engagement.

Blockchain-enabled smart contracts provide a secure and transparent environment for managing consent and enforcing privacy rules (Chang, Chen, Lu, & Luo, 2020). By leveraging blockchain's immutable audit trails, the framework ensures compliance with privacy regulations while enhancing user trust (Merlec, Lee, Hong, & In, 2021; Gomez-Trujillo, Velez-Ocampo, & Gonzalez-Perez, 2021). This multifaceted approach addresses the technical and ethical challenges of current systems and also creates a scalable, user-centered model for privacy preservation in smart home healthcare.

Table 2. 4: Potential for Integrating Blockchain, AI, and User-Centric Strategies

Technology/ Approach	Potential	Research Opportunities
Blockchain	Enhancing data privacy and security in IoT environments	Developing lightweight blockchain protocols for resource-constrained devices Exploring novel consensus mechanisms for IoT networks
AI-Driven Privacy Management	Sophisticated privacy risk assessment and automated policy enforcement	Developing AI models for privacy risk assessment Implementing automated privacy policy enforcement Exploring federated learning and edge AI for privacy-preserving analytics
Adaptive User-Centric Privacy Frameworks	Personalised privacy protection with minimal user burden	Developing frameworks that learn from user behaviors and preferences Creating adaptive privacy systems that adjust over time Balancing comprehensive privacy controls with ease of use

2.9 Discussion and Conclusion

This literature review has critically examined the landscape of privacy preservation in SHHE, highlighting the challenges, limitations, and opportunities within this rapidly evolving field. The integration of IoT technologies into healthcare systems has introduced transformative possibilities for personalised and efficient care, particularly for aging populations and individuals with chronic conditions. However, the sensitive nature of healthcare data, combined with the complexity of smart home environments, underscores the need for robust privacy-preserving frameworks to address growing concerns about data security and user trust.

Key findings reveal that while traditional privacy-preserving schemes such as anonymisation, encryption, and differential privacy, offer a foundational layer of data protection, they fall short in terms of scalability, interoperability, and adaptability to user preferences. Context-aware models that incorporate time-decay factors, role-based access control, and sensitivity-based data handling have emerged as promising approaches to address some of these gaps. However, their implementation remains challenging due to technical complexity and limited real-world applicability. Emerging technologies, such as blockchain and AI, hold significant potential for enhancing privacy and security, yet they introduce challenges related to computational overhead and ethical considerations.

The findings also emphasise the critical importance of user-centric designs, which empower users with greater control over their data through dynamic consent management and transparency mechanisms. Ethical considerations, including fairness, data ownership, and informed consent, remain underexplored in current models, further highlighting the need for holistic frameworks that integrate technical solutions with normative principles.

Despite advancements, this review identifies several persistent gaps in existing privacy-preserving technologies. Scalability remains a pressing issue as the volume of data generated by IoT devices continues to grow. Interoperability across heterogeneous devices and platforms is insufficiently addressed, leading to inconsistent privacy protections. Furthermore, computational overhead limits the applicability of advanced privacy techniques in resource-constrained environments. Ethical integration and user-friendly interfaces are also lacking in many existing models, reducing their effectiveness and user acceptance. Current evaluation frameworks often rely on synthetic data and controlled environments, which fail to capture the complexities of real-world scenarios. Table 2.5 summarises the key findings and gaps identified in this review, providing a comprehensive overview of the challenges and opportunities in SHHE privacy preservation.

This review underscores the urgent need for a novel approach that seamlessly integrates emerging technologies, user-centric design principles, and ethical considerations. Such an approach should balance data utility with privacy protection, address scalability and interoperability challenges, and empower users through transparency and control. The proposed research builds on these findings by introducing a consent-centric privacy model,

where the smart contract is designed based on the Dynamic Privacy Score Model (DPSM) for adaptive privacy score computation and the Multi-Dimensional Dynamic Consent (MDDC) model for flexible, context-aware data governance. Additionally, it incorporates sophisticated privacy risk assessment and automated policy enforcement mechanisms, leveraging ML-driven analytics to enhance security, compliance, and real-time decision-making. This integration ensures automated, user-centric data management while maintaining transparency, security, and compliance with privacy regulations. Future research will focus on validating these solutions in real-world settings to ensure their practical applicability and effectiveness in enhancing privacy and security in SHHE.

By addressing these gaps, the research aims to advance the development of adaptable, robust, and ethically sound privacy-preserving frameworks for smart home healthcare systems, setting a foundation for secure and trustworthy healthcare technologies.

Table 2. 5: Summary of Background Research

Theme	Key Findings	Gaps Identified
Evolution of Smart Home Technologies	***Significant growth and adoption are projected by 2025*** (Statista; Insights, 2024; Research, 2018); ***IoT market expansion to 75 billion devices*** (Butun, Sari, & Österberg, 2019)	***Need for scalable solutions to handle increasing data volumes*** (Iqbal, et al., 2021).
Privacy and Security Challenges	***Unauthorised access*** (Ogonji, Okeyo, & Wafula, 2020; Alaba, Othman, Hashem, & Alotaibi, 2017), ***IoT device vulnerabilities*** (Bugeja, Jacobsson, & Davidsson, 2016; Ali, Dustgeer, Awais, & Shah, 2017), ***ethical concerns*** (Zyskind & Nathan, 2015).	***Interoperability*** (Sousa, Mendonça, & Machado, 2022; Egala, Pradhan, Badarla, & Mohanty, 2021) ***and computational overhead*** (Ma, Naas, Sigg, & Lyu, 2022; Nasir, et al., 2022).
Existing Privacy Preservation Schemes	***Anonymisation*** (Hossain, 2016), encryption (Dhanda, Singh, & Jindal, 2020; Surya, Ranichandra, & Ranjani, 2018), ***differential privacy*** (Jayaraman & Evans, 2019; Bun & Steinke, 2016), ***transparency*** (Bergram, Bezençon, Maingot, Gjerlufsen, & Holzer, 2020; Aqeel, et al., 2022).	***Scalability*** (Zyskind & Nathan, 2015; Xiao & Xiong, 2015), ***user-centric design*** (Mehta, Gooch, Bandara, Price, & Nuseibeh, 2021; Anom, 2020)***, ethical integration*** (Hummel, Braun, & Dabrock, 2021; Mosquera-Lopez, et al., 2020). ***Scalability, user-centric design, adaptability, context-awareness*** (Belguith et al., 2020; Hossein et al., 2019, 2021)
Context-aware Privacy Models	***Time-decay factors*** (Sylla, Chalouf, Krief, & Samaké, 2021; Luo, et al., 2018), ***role-based access control*** (Chen, et al., 2018; Ameer, Benson, & Sandhu, 2022), ***and sensitivity-based handling*** (Morrison, 2016; Kumar, Braud, Kwon, & Hui, 2020).	***Implementation complexity*** (Al-Sharhan, Omran, & Lari, 2019; Suriyakumar, Papernot, Goldenberg, & Ghassemi, 2021) ***and real-world applicability*** (Irshad, et al., 2023; Altherwi, et al., 2024).
User Consent and Ethical Data Disclosure	***Dynamic consent management*** (Burkhardt, Boy, Doneddu, & Hajli, 2023; Muravyeva, Janssen, Specht, & Custers, 2020), ***data minimisation*** (Yusupova & Ismailov, 2023; Adeniyi, Arowoogun, Okolo, Chidi, & Babawarun, 2024), ***transparency*** (Sharma, Chen, & Sheth, 2018).	***Comprehensive ethical integration*** (Yuvaraj, Praghash, & Karthikeyan, 2022; Felber, Tian, Pageau, Elger, & Wangmo, 2023) ***and user-friendly interfaces*** (Wickramasinghe & Reinhardt, 2021; Wickramasinghe, 2022).
Proposed Enhancements and Innovations	***Consent-centric models*** (Rahman, Hasan, Rahman, & Momotaj, 2024; Kounoudes & Kapitsaki, 2020), smart contracts (Liu, Zhang, Wan, Ji, & Tian, 2020; Chang, Chen, Lu, & Luo, 2020), ***and dynamic privacy score***s (Patel & Jadhav, 2024; Merlec, Lee, Hong, & In, 2021) ***Adaptive privacy risk assessment***.	***Robust validation and evaluation in real-world settings*** (Mosquera-Lopez, et al., 2020; Silva, Gonçalves, Antunes, Curado, & Walek, 2022), ***ML-enhanced privacy preservation and system optimisation.***

Chapter 3

3. Methodology for Privacy-Aware Authorisation Framework

This chapter addresses the need for a robust, user-centric system that ensures the privacy and security of sensitive health data while enabling authorized data sharing. It presents the methodology for developing a privacy-aware authorisation framework, focusing on ethical information disclosure, privacy model design, and validation processes.

3.1 Introduction

This section provides an overview of the research context, presenting the necessity of a privacy-aware authorisation framework within smart home healthcare environments. This introduction highlights the growing importance of ethical data handling and user consent, especially considering the increasing integration of IoT devices for personal health data collection.

The research is centered on addressing challenges related to the ethical disclosure of sensitive data in these environments. A consent-centric privacy model is designed to provide users with granular control over their health data, incorporating dynamic privacy preferences. The methodology aligns with the key objectives of ethical data disclosure, dynamic user consent management, and the development of adaptive privacy scoring mechanisms to adjust according to individual preferences. The chapter proceeds by detailing the research approach, methodology, and frameworks used to address the privacy and security challenges inherent in this context. Key research objectives include:

1. Ethical data disclosure within healthcare systems.
2. Dynamic user consent management through blockchain technology.
3. Adaptive privacy scoring mechanisms that adjust according to user preferences.

The research adopts a longitudinal time horizon, designed to capture changes in user behavior and system performance over an extended period. This approach ensures that the privacy model remains adaptable, effective, and relevant under real-world conditions while accommodating potential variations in system interaction. The model also integrates machine learning (ML) for privacy risk assessment, providing continuous feedback to the smart contract and privacy model design, allowing for system refinement as emerging privacy concerns are detected.

An agile prototyping approach underpins system development, emphasising iterative cycles of prototyping, feedback collection, and continuous refinement. The PADDI methodology (Plan, Analyze, Design, Develop, Implement) guides the development of the smart contract-based authorisation framework, ensuring that the system's components evolve based on user feedback and changing privacy considerations. This iterative improvement process utilised adopts the agile approach, ensuring that continuous user involvement and feedback loops are integral to the system's development and optimisation.

Figure 3.1 illustrates the methodology employed in this research, showing the iterative process of developing the privacy-aware authorisation framework. It highlights the flow from survey methodology and data collection to privacy model design, with a feedback loop that enables continuous refinement based on user input. The integration of machine learning (ML) for privacy risk assessment allows for feedback to both the smart contract implementation and the privacy model design, facilitating updates to the smart contract logic through an upgradable contract pattern, which maintains blockchain immutability while adapting to emerging privacy concerns. This ML-driven feedback mechanism, as elaborated in Chapter 7, supports anomaly detection while simultaneously improving the system's adaptability through its influence on the Dynamic Privacy Scoring Model (DPSM), the Multi-Dimensional Dynamic Consent (MDDC) model, and the enforcement logic embedded in smart contracts.

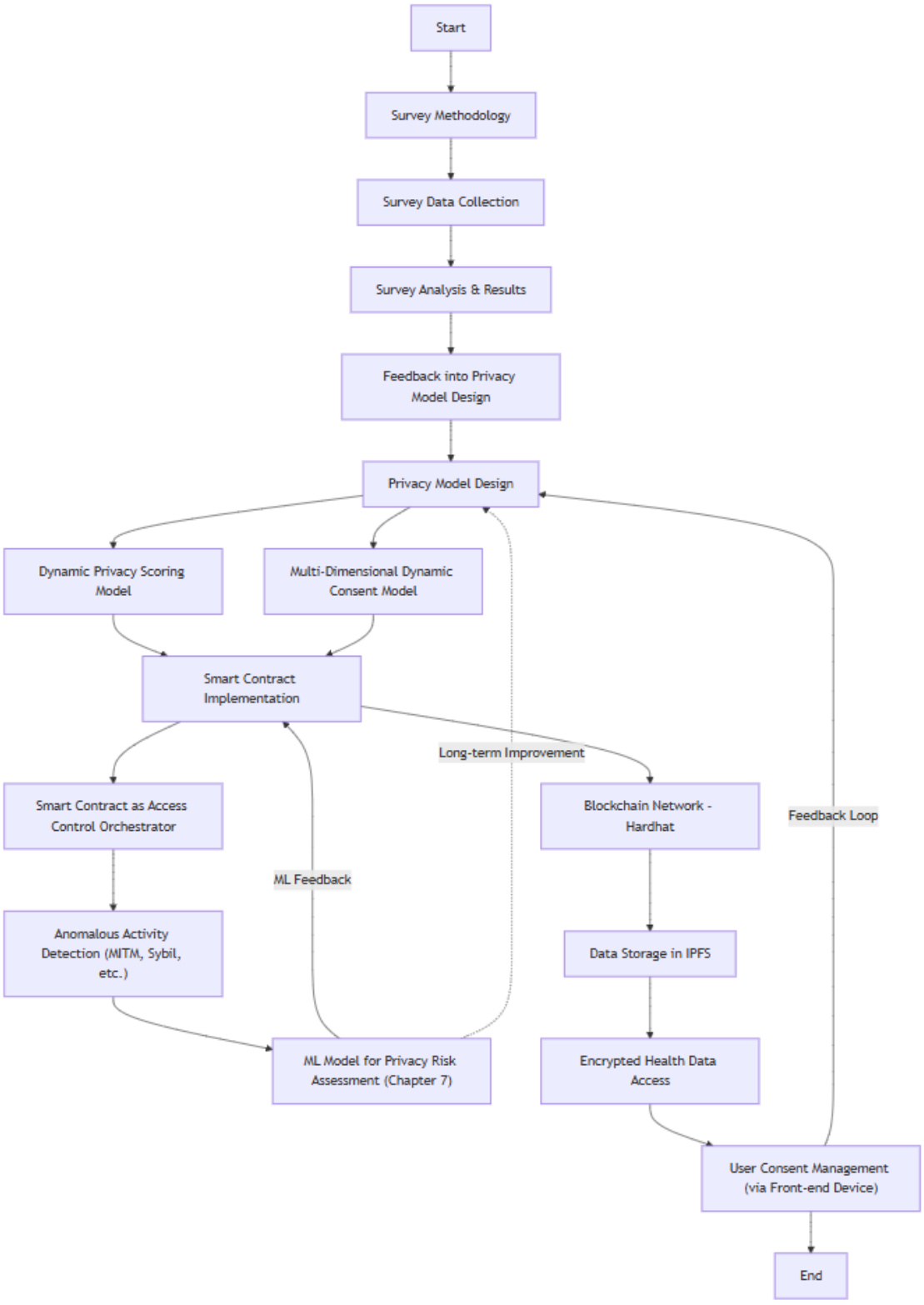


Figure 3. 1: Flow Diagram for the Proposed Privacy-Aware Authorisation Framework

3.2 Research Design and Approach

This outlines the research design and approach adopted for this study, justifying the chosen methodology and providing an overview of the research process. The research design utilised the Saunders Research Onion framework, which offers a comprehensive and systematic design approach to research methodology (Melnikovas, 2018; Seuring et al., 2021). The framework is also chosen for its ability to provide a holistic view of the research process, allowing for the integration of various methodological elements that are crucial for addressing the research objectives. The complex nature of developing an ethical information disclosure and privacy model for smart home healthcare systems necessitates a multifaceted research approach (Ahmadi-Assalemi, et al., 2020). This framework will guide and also inform the approach taken in subsequent sections of this chapter.

The systematic research design approach, outlined in Table 3.1, summarises the layers of the Saunders Research Onion applied to this study. It provides a comprehensive overview of the chosen methodology, which aligns with the key objectives of this research.

Table 3. 1: Systematic Research Design Approach for Privacy-Aware Authorisation Framework

Research Design Layer	Type Chosen	Description
Research Philosophy	Pragmatism	Focuses on practical solutions, combining both qualitative and quantitative perspectives to address privacy and security in healthcare systems.
Research Approach	Deductive	The approach moves from general theories to specific observations related to privacy and ethical data management in smart homes.
Methodological Choice	Mixed Methods	Combines both qualitative (user feedback, expert evaluations) and quantitative (system performance, privacy scores) data to validate the privacy model.
Research Strategy	Experiment, Action Research, Case Study	Used to gather insights and validate the framework in real-world settings through a testbed environment incorporating IoT devices and blockchain infrastructure.
Time Horizon	Longitudinal	Designed to observe changes in user behavior and system performance over an extended period, ensuring the adaptability of the privacy model.
Data Collection	System logs, surveys, user evaluations	Data is gathered through surveys, real-time system logs, and user evaluations to assess privacy preferences and model effectiveness in a healthcare setting.
Data Analysis	Statistical, Thematic, Privacy Score Computations	Includes analysis of system logs, privacy scores, user feedback, and machine learning models used for privacy risk assessment and predictive modeling.
Validation Techniques	Performance evaluation, privacy & security, user evaluation	Ensures the model's effectiveness through performance testing, security checks, and user satisfaction surveys. Details are provided in Chapter 6.
Tools, Techniques, and Development Environment	As listed in Table 3.1	Includes hardware specifications (e.g., IoT devices, cloud servers) and software environments (e.g., Solidity, TensorFlow, Hardhat) used to implement the privacy model.

3.2.1 Overview of the Research Process

Research Philosophy: The research process is guided by a pragmatic philosophy, focusing on practical solutions and real-world applications in the context of ethical information disclosure and privacy in smart home healthcare systems. This pragmatic approach allows for the combination of both objective and subjective viewpoints, integrating different perspectives to address the research problem effectively.

Research Approach: The deductive approach employed in this study facilitates hypothesis testing based on existing theories and literature, particularly concerning privacy and ethical data management in smart home environments. This approach transitions from general theories to specific observations and findings related to the proposed privacy model.

Methodological Choice: The study adopts a mixed-methods approach, combining qualitative feedback (from users) and quantitative analysis (privacy scores, system performance) to validate the privacy model. A key aspect of this methodological approach is its focus on comprehensive privacy model validation. This involves the integration of quantitative analyses, such as privacy scores and system performance metrics, with qualitative assessments of user experiences and privacy preferences. By combining numerical and experiential data, this approach ensures robust validation of the proposed privacy framework. Quantitative data are gathered through system logs, performance metrics, and privacy scores, while qualitative data are derived from user feedback, expert evaluations, and usability assessments. The integration of these diverse data types offers a deeper understanding of both the technical effectiveness of the system and user acceptance of the privacy model. Ethical objectives, such as privacy protection and user empowerment, are addressed by integrating analyses of privacy mechanisms and their practical impact. This comprehensive approach ensures that the technical and ethical dimensions of the privacy-preserving framework are thoroughly evaluated.

Research Strategy: A combination of experiment, action research, and case study approaches is used to gather insights and validate the privacy framework in real-world settings. A thoroughly designed test bed environment served as the foundation for these strategies, incorporating IoT devices, server infrastructure, and network components. This testbed enabled the collection of real-world data while maintaining controlled conditions to evaluate the proposed privacy-preserving authorisation framework.

3.3 Data Collection and Analysis

Data collection is conducted through surveys, system logs, and user evaluations to capture privacy preferences and usability concerns. The data collection methods allow us to validate the effectiveness of the privacy model in real-time healthcare settings. The survey instrument is designed to assess user perceptions regarding privacy preferences, role-based access, and data sensitivity. In this study, data is collected through:

- *System Logs*: System logs will record access control decisions, enabling the analysis of privacy breaches and security risks.
- *Survey Data*: Feedback is gathered on user preferences for data sharing, focusing on time-decay, role-based weight, and data sensitivity.

The experimental setup was organised into three main components: data collection infrastructure, processing and management layer, and analysis and validation components. These elements were designed to work together seamlessly, enabling systematic data collection and validation while maintaining controlled conditions for testing the privacy-preserving mechanisms. Data analysis procedures include statistical analysis, thematic analysis, and privacy score computations. Transactional data procedures in Chapter 5 were further evaluated in Chapter 6. Table 3.2 and Figure 3.2 illustrate the structure and functionality of this setup, providing a visual representation of its key elements and their roles in achieving the research objectives.

Table 3. 2: Technical Infrastructure and Development Environment Specifications for the Privacy-Aware Authorisation Framework

Component Category	Component	Details
IoT Devices	Sensors & Hardware	- Raspberry Pi 4 Model B, Quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz, 4GB RAM - Enviro+ Air Quality (PIM 458) pHAT for environmental monitoring - Wearable Health Sensors (e.g., smartwatches - Samsung Galaxy Watch 4)
Network Infrastructure	Networking Components	- Wireless Router (450Mbps N router) - Home Gateway for data aggregation and initial encryption
IoT Clients & Server	Hardware & OS	- Raspberry Pi OS (for Raspberry Pi devices) - Cloud Database Server - Intel Core i7-6700K CPU@ 3.40GHz, 16GB DDR4 RAM, 1TB SSD - Ubuntu 22.04 LTS
Development Environment	IDE & Tools	- Visual Studio Code 1.78 - Hardhat Development Environment v2.14.0 - Node.js v18.17.1 -cURL Tool v 1.12.2
Programming Languages & Frameworks	Backend	- Python 3.7 and 3.8 - Solidity v0.8.0 - Node.js Runtime - NPM 9.6.7
	Frontend	- React v18.2.0 - JavaScript ES6+; v.1.8.5
Blockchain Infrastructure	Network	- Ethereum (Hardhat 2.14.0 Network for development) - MetaMask v10.28.1 (Wallet & Authentication Tool); for deploying and testing Ethereum smart contracts)
	Smart Contracts	- Solidity v0.8.21 - Hardhat for deployment - Ethers.js v5.7.2 for interaction - Proxy contract pattern for upgradable contracts
Storage Solutions	On-chain	- Ethereum Smart Contracts - Contract Storage for access control logic
	Off-chain	- IPFS for distributed data storage - Spreadsheet: Excel
Development Tools	Testing & Deployment	- Hardhat 2.14.0 Testing Framework - Chai for assertions - Ethereum Waffle for smart contract testing
Security Libraries	Cryptography	- PyCryptodome (for implementing AES and ECC encryption) - Web3.js for blockchain interactions Ethers 6.0.0
Machine Learning	Anomaly & Privacy Violation Detection	- scikit-learn (for anomaly detection and machine learning) - TensorFlow and Keras (for model training in privacy violation detection)
Predictive Privacy Risk Assessment	Privacy Risk Models	- Ensemble Random Forest & Extra Tree Classifier for predictive privacy risk assessment - R^2, Mean Squared Error (MSE), and confusion matrix to evaluate model performance
Adaptive Privacy Scoring Mechanisms	Dynamic Privacy Model	- Solidity for creating adaptive smart contracts - Ethereum blockchain for dynamic privacy scoring adjustments - IPFS for off-chain privacy-related data storage

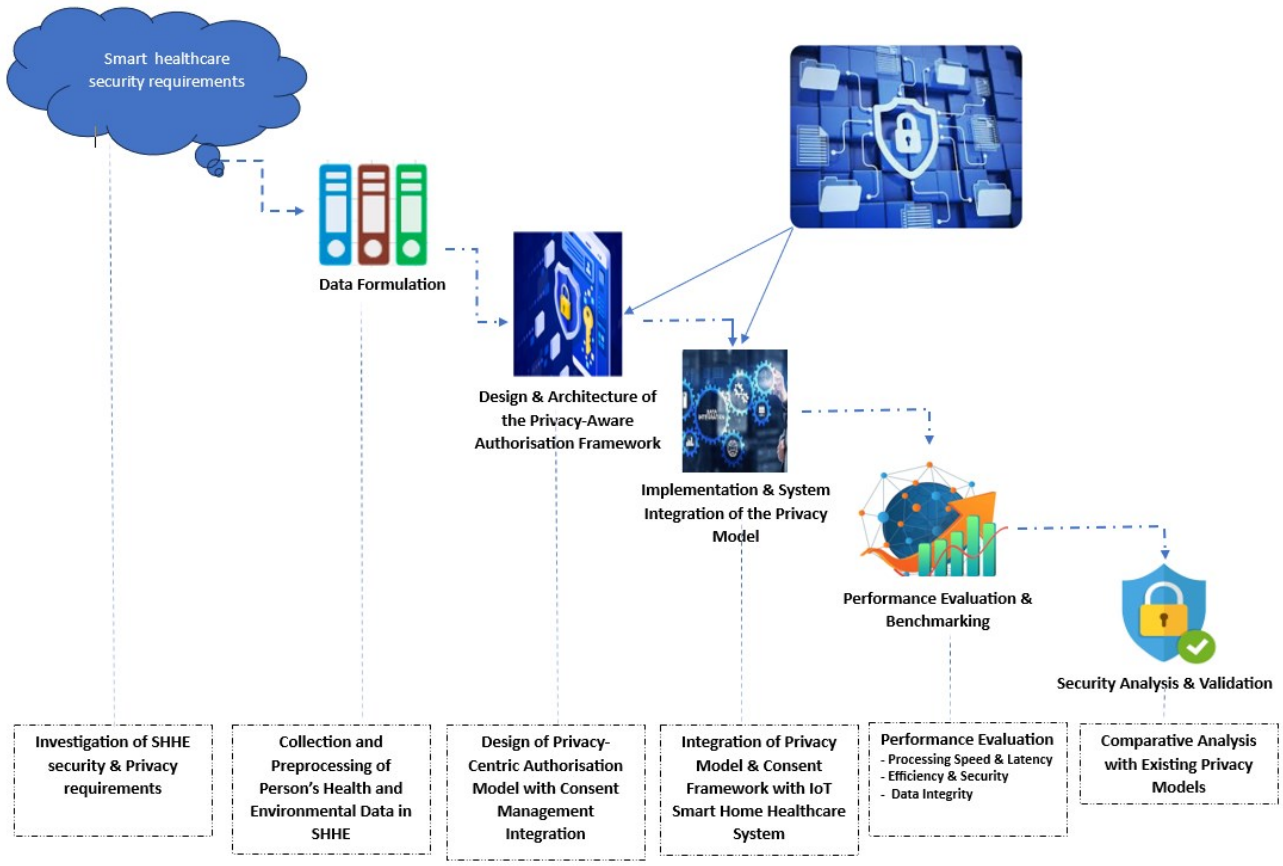


Figure 3. 2: Research Methodology Flow for Framework Development in SHHE

The research methodology illustrated in Figure 3.2 guided the study's systematic data collection, processing, and evaluation. The study implemented an experimental architecture that established a comprehensive smart home healthcare ecosystem, enabling secure health data sharing through the integration of IoT devices, smart contracts, IPFS storage, and blockchain networks. This controlled environment facilitated the generation of empirical data and validation of the proposed privacy model, forming the foundation for the four key contributions to knowledge presented in this thesis. These contributions address critical aspects of privacy-aware access control, consent management, temporal dynamics of privacy, user preferences and system acceptance, and predictive privacy risk assessment.

3.4 Privacy Model Development and HealthDataSharing System

This section presents the methodological choice for developing a comprehensive privacy-aware authorisation framework, particularly focusing on the HealthDataSharing System employed as a case study within smart home healthcare ecosystems. The HealthDataSharing System exemplifies the integration of user-centric privacy management into healthcare data sharing by combining blockchain technology, smart contracts, and dynamic privacy scoring.

Central to this model are defined actors a.k.a stakeholders with the SHHE e.g., patients, healthcare providers, family members, and research institute, each with specific roles and responsibilities influencing access control decisions, privacy scoring, and consent management. Healthcare providers or experts request data access governed by Role-Based Access Control (RBAC) integrated with dynamic privacy scores. Patients manage consent via front-end interfaces, dynamically adjusting access permissions based on preferences and data sensitivity. The smart contract ensures that the configured system policies align with evolving privacy requirements. To visually represent the system interactions and structural design, two key diagrams are presented. In Figure 3.3, the use case diagram shows interactions between system actors (i.e., stakeholders) and core functionalities within the HealthDataSharing System built on Ethereum. The patient manages data access and privacy preferences, while IoT devices upload encrypted data to IPFS, recording hashes on a Blockchain. Healthcare providers retrieve and decrypt data, and research institutes analyse anonymised data for research. Family members receive event notifications to support patient care.

Figure 3.4 illustrates the Class Diagram, detailing the HealthDataSharing system's data structure, stakeholder interactions, and blockchain integration. It includes classes such as Patient (managing permissions), HealthData (encrypted data storage), and IPFSHash (linking stored data to blockchain records). AccessControl manages permissions granted to healthcare providers, research institutes, and family members. EncryptionDetails ensures cryptographic security across data-sharing activities and the interactions underpinning privacy and security operations. These diagrams offer clear insights into actor interactions and data governance structures, ensuring a transparent, auditable, and user-controlled privacy management

environment. The design concepts for the actors within the HealthDataSharing System and their functionalities are fully explained in subsection 4.1.1. (chapter 4).

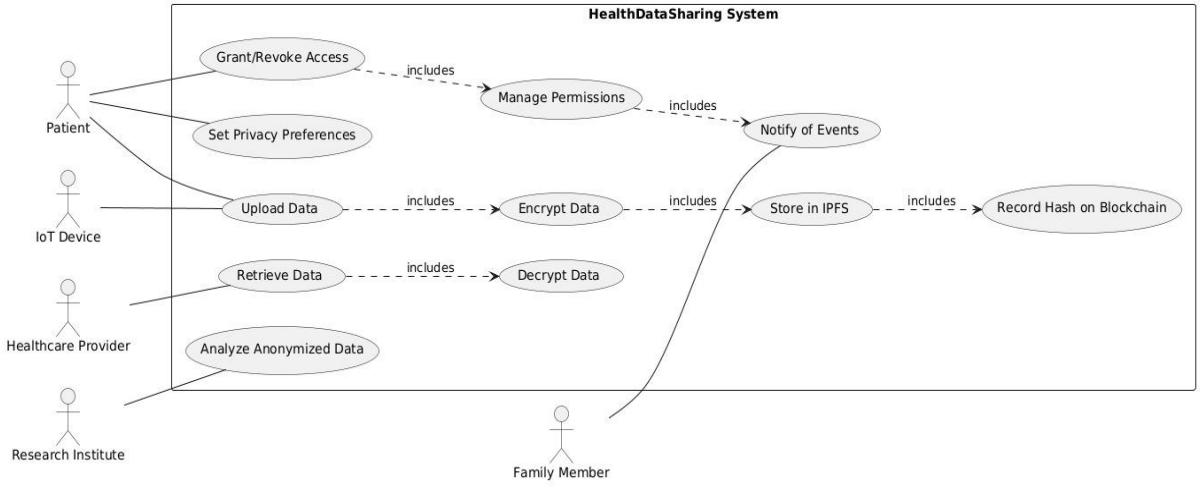


Figure 3. 3: Use Case Diagram of the HealthDataSharing System

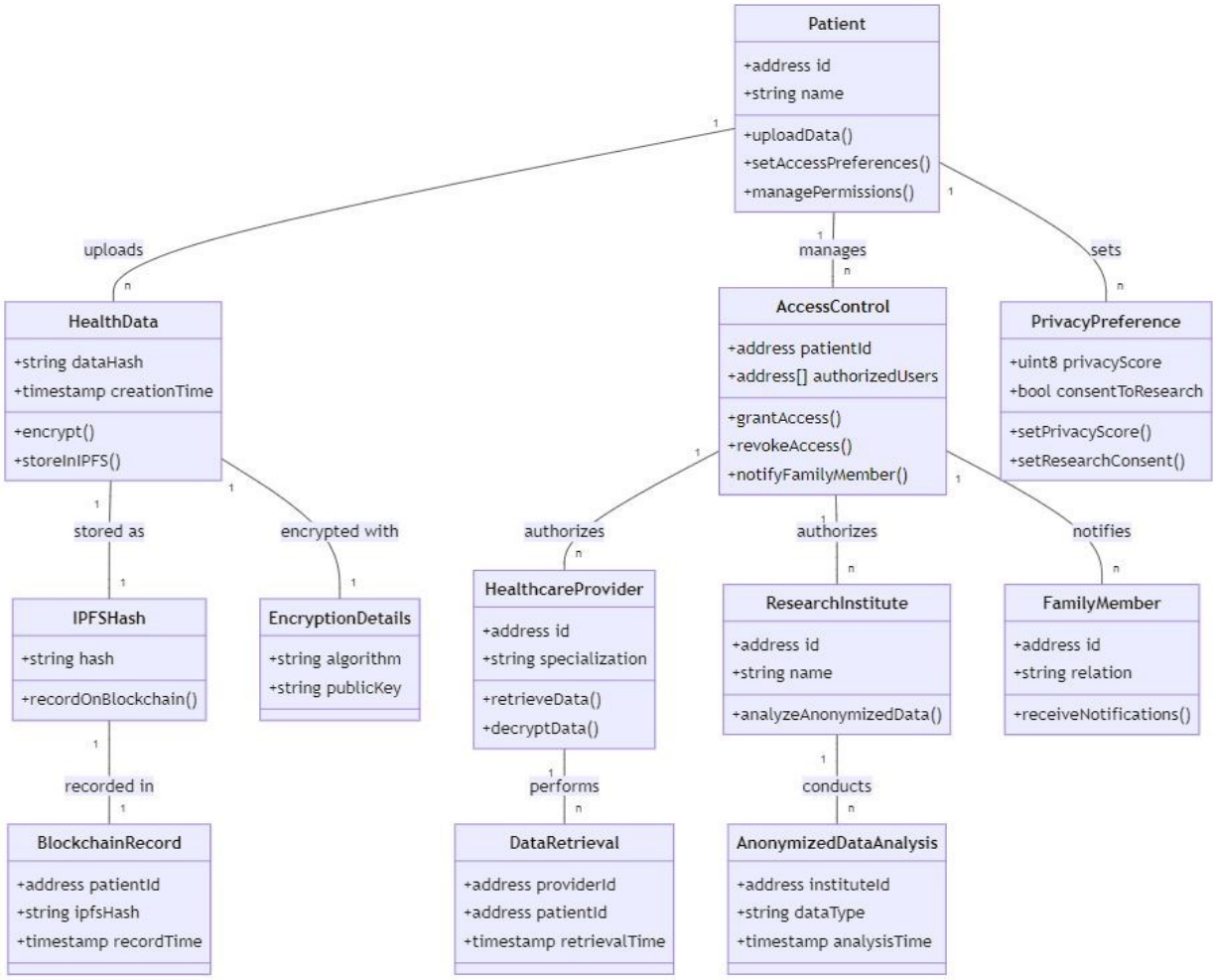


Figure 3. 4: Class Diagram of the HealthDataSharing System Architecture

The development approach integrates dynamic privacy scoring based on the Time-Decay Factor (TDF), Role-Based Weight Factor (RBWF), and Data Sensitivity Factor (DSF), addressing limitations in traditional privacy models such as lack of adaptability to evolving healthcare data access patterns. This methodological choice enhances context awareness, aligns data sensitivity with user-defined preferences, and facilitates responsive privacy management through blockchain-enabled smart contracts.

The privacy model leverages user feedback loops and machine learning (ML)-driven insights, dynamically refining access control mechanisms. This ensures continuous adaptation to emerging privacy threats and evolving user expectations, providing both robust protection and user-centric flexibility in healthcare data sharing.

3.4.1 Core Components of the Privacy Model

Building on Acquisti, Taylor, and Wagman (2016) principle of privacy as control over data sharing, the privacy model proposed in this study is built upon three core components i.e., TDF, RBWF & DSF that govern access decisions and provide a nuanced approach to privacy management. These three work together to create a dynamic and context-aware privacy protection system. Each of these factors is examined in detail.

The privacy model developed integrates three core components to ensure adaptability and granularity in privacy decisions, addressing user-centric privacy preferences within healthcare data sharing contexts. The values assigned in each component are constrained between 0 and 1 to align with the sigmoid function utilised for normalising decision outcomes, facilitating seamless integration with the model's binary access control decisions (allow: 1, deny: 0). This choice leverages the sigmoid function's characteristics of providing a smooth gradient useful in logistic regression and decision-based systems, particularly suitable for squashing linear combinations of weighted inputs into probabilistic outputs ranging strictly between 0 and 1 (Zyskind et al., 2015).

3.4.1.1 Time-Decay Factor (λ)

The TDF (λ) reflects the temporal sensitivity of data and accounts for how its relevance diminishes over time. Data is categorised into three time-based classes to demonstrate the possible range of data recency:

1. Latest data (Cat 1: 0-30 days): Highest relevance and sensitivity = 0.9
2. Recent data (Cat 2: 31-90 days): Moderate relevance and sensitivity = 0.7
3. Earlier data (Cat 3: >90 days): Lower relevance and sensitivity = 0.5

These three time-based categories are justified based on healthcare data relevance (Miao, Ding, & Wu, 2022), access control policies, and privacy-preserving frameworks. The highest sensitivity is assigned to recent data (0-30 days) due to its immediate importance in patient care (Impiö, Yamaç, & Raitoharju, 2021). Moderately aged data (31-90 days) retains value for ongoing treatments, while older data (>90 days) is typically used for historical reference and research, justifying a lower sensitivity score. These classifications align with best practices in privacy-aware healthcare data management and temporal access control frameworks (Abbasi & Smith, 2024). These categories ensure that recent data is more heavily weighted during

privacy score computation, reflecting its increased sensitivity in the context of healthcare systems.

The Time-Decay Factor (TDF) dynamically adjusts privacy scores based on data relevance over time, reflecting the decreasing utility and sensitivity of data as it ages. Data relevance, and consequently privacy risk, diminish as data become older, represented mathematically and modeled as a time-decay function in equation (1):

$$\lambda(t) = e^{-\alpha(T-t)} \quad (1)$$

Where:

- the decay rate λ is selected based on domain-specific privacy requirements and user-defined preferences. This ensures that recent data, inherently more sensitive, receives greater privacy protection.
- t is the current time
- T is the data arrival time
- α is the decay constant determined through user studies and expert input

This function assigns higher weights to more recent data actions and lower weights to older actions, reflecting the importance of data recency in privacy score calculation. This is expected to allow for customisation, where users can adjust the decay rate (α) and time categories through an intuitive front-end application, allowing for personalised time-sensitivity preferences.

3.4.1.2 Role-Based Weight Factor (ω_r)

The RBWF(ω_r) differentiates data consumers based on their roles, assigning trust-based weights that regulate data access. This factor aligns with the principle of least privilege (Cawthra, et al., 2022), ensuring that data access is commensurate with the user's role in the healthcare ecosystem.

The RBWF assigns differentiated access weights based on the specific roles of data consumers. Roles are categorised with values within the [0, 1] interval to provide varying degrees of access control granularity. Table 3.3 illustrates these weights, for example:

- Healthcare Providers: $\omega_r = 0.9$ (reflecting high access necessity for Direct Carers)
- Family Members: $\omega_r = 0.7$ (moderate access necessity for Secondary Carers)
- Researchers: $\omega_r = 0.5$ (conditional moderate access necessity)

- Third-party Vendors: $\omega_r = 0.3$ (e.g., restricted access necessity health insurance entities)

These values reflect trust levels and the necessity for access derived empirically through user feedback and expert validation within healthcare contexts, ensuring fine-grained privacy management.

These weights are commensurate with the user's role in the healthcare ecosystem, ensuring that roles with higher levels of trust, such as doctors, receive greater access privileges. These initial values are flexible and can be adjusted based on user preferences and regulatory requirements. By aligning with the principle of least privilege, these weights ensure that data access reflects the user's role while supporting personalised preferences. The frontend application facilitates the adjustment of these weights, allowing for customised role-based access control in the system.

3.4.2.3 Data Sensitivity Factor (γ_d)

The Data Sensitivity Factor (DSF) allows users to set privacy preferences based explicitly on the intrinsic sensitivity of various healthcare data categories by setting a privacy benchmark through a privacy preference policy. This factor allows for the personalisation of privacy settings based on individual user concerns and the nature of the data being shared. Sensitivity values are bounded between 0 and 1, again aligning with the sigmoid normalisation employed.

For implementation, the three sensitivity levels as shown in Table 3.3 are defined:

1. High sensitivity (e.g., critical health records, chronic conditions): $\gamma_d = 0.9$
2. Sensitive personal data (e.g., medication details): $\gamma d = 0.7$
3. Moderate sensitivity (e.g., lifestyle data, routine check-up data): $\gamma_d = 0.5$
4. Low sensitivity (e.g., environmental data, activity data): $\gamma_d = 0.3$

This classification supports nuanced and user-driven privacy protection decisions tailored to specific types of healthcare data.

The data sensitivity function is modeled as:

$$\gamma_d = \frac{1}{1 + e^{-\beta(x - x_0)}} \quad (2)$$

Where:

- x is the sensitivity level

- β is the sensitivity constant
- X_0 is the threshold

Users will be able to adjust these sensitivity levels through the frontend application, allowing for granular control over their privacy preferences for different types of data.

To illustrate the interaction between sensitivity levels and the Role-Based Weight Factor, a decision matrix approach is proposed as shown in Table 3.3 to provide an example of this interaction, where each user role and data type are assigned a sensitivity weight based on user preferences and regulatory requirements.

Table 3. 3: Illustrative examples of Data Classification and Assigned Values

Data Item	**Sensitivity Weight (γd)**	**Role: Doctor (ω_r)**	**Role: Family Member (ω_r)**	**Role: Researcher (ω_r)**
Medical History	0.9	0.9	0.7	0.5
Medication	0.7	0.7	0.5	0.3
Lifestyle Data	0.5	0.6	0.5	0.2
Environmental Data	0.3	0.5	0.4	0.2

These core components collectively operationalise a robust, adaptive privacy model capable of responding dynamically to evolving privacy needs and healthcare data usage scenarios, enabling precision in ethical data disclosure decisions.

These factors enable the system to prioritise sensitive data, ensuring granular control over access decisions. These components collectively enable a static computation of the privacy score, deduced from the linear function proposed in the study by Psychoula (2020) and presented in Equation 3:

$$P = \lambda(t) \times \omega_r \times \gamma_d \quad (3)$$

3.4.2 Dynamic Privacy Score Computation

The dynamic nature of the privacy scoring system addresses privacy management challenges by integrating behavioral adjustments based on historical interactions (Branscomb, 1994; Nissenbaum, 2020). The privacy score is calculated as a function of these three factors. The dynamic privacy score extends static computations by incorporating time sensitivity, role significance, and data sensitivity factors (TDF, RBWF, and DSF). This score dynamically

reflects the privacy level based on accumulated actions, adjusted for time relevance, role significance, and data sensitivity as depicted in Figure 3.5. Hence, a dynamic privacy score mathematical model was deduced from the study by (Zyskind & Nathan, 2015).

The dynamic privacy score P for a user i at interaction instance n is computed using:

$$P_n^{(i)} = \frac{1}{1 + e^{-\alpha(\sum_{t=0}^{T} \lambda^{T-t} \omega_r \gamma_d (allow_t - deny_t))}} \quad (4)$$

Where:

- i : Identifier for a specific user.
- n : Current interaction instance or access request.
- $\lambda^{(T-t)}$: Cumulative interaction history
- $allow_t$ - $deny_t$: Cumulative count of previously allowed and denied access requests at time t.
- ω_r : Role-based weight reflecting access privilege levels
- γ_d: Data sensitivity factor, scaling scores based on data importance
- α: Sensitivity constant controlling the impact of historical data

This equation dynamically adjusts privacy scores based on historical interactions i.e., reflecting the cumulative behavior of users and their historical trustworthiness, and providing context-aware privacy management.

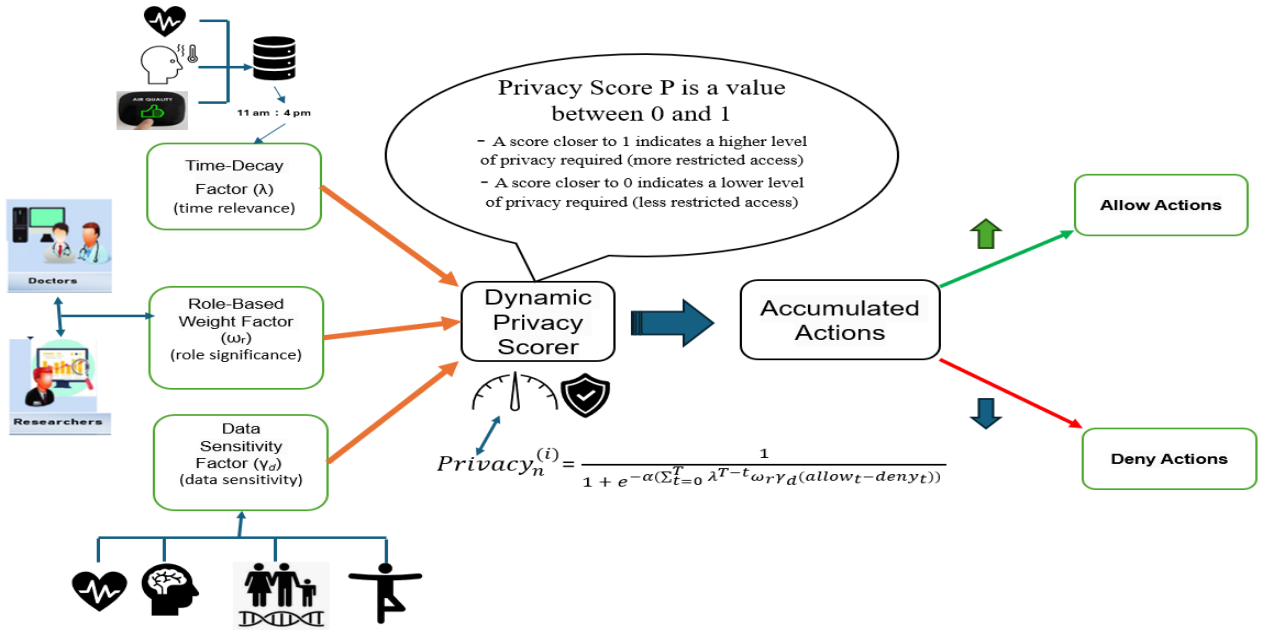


Figure 3. 5: Underlying Operational Model of Privacy Scoring in the HealthDataSharing System.

The computed privacy score ranges between 0 and 1; higher values indicate greater restriction levels. This provides a clear measure of the level of privacy required based on the sensitivity of the request.

Dynamic Nature: The privacy score adapts dynamically to context. As time passes, $\lambda(t)$ decreases, lowering scores for older data. Role-based weights (ω_r) and data sensitivity factors (γ_d) further influence the score, ensuring it reflects both the user's role and the data type's sensitivity.

Threshold-Based Access Control*:* Threshold values determine access control such that;

- $P \geq 0.7$: Explicit user consent required.
- $0.4 \leq P < 0.70$: May require additional authentication.
- $P < 0.4$: Standard access allowed.

However, scenarios involving repeated denials or approvals may arise from specific patient contexts, emergencies, or perceived privacy violations. To manage such scenarios effectively, an adaptive, ML-driven risk assessment mechanism (discussed in Chapter 7) dynamically evaluates access patterns, proactively identifying and mitigating anomalous or suspicious activities. The integration of this machine learning-driven privacy optimisation framework ensures the accurate detection of false positives and negatives in access control decisions, thus reducing unauthorised access risks. Furthermore, threshold settings are personalised via an intuitive frontend, enabling real-time behavioural adjustments that enhance both security and usability.

Integration with Ethereum Blockchain**:** The decision to employ an Ethereum blockchain-based approach is justified by the inherent advantages of smart contracts as programmable, secure, and automated access-control mechanisms. Ethereum is notably recognized as the pioneering platform for smart contract implementation, and while other blockchain platforms exist, Ethereum remains the most widely adopted due to its robust smart contract functionality, well-established developer community, and mature ecosystem. These characteristics ensure transparency via auditable transaction logs, and immutability by securely preserving historical computations and automating the enforcement of access control decisions. Hence, the designed smart contracts modeled around the Dynamic Privacy Scoring Model (DPSM) and the Multi-Dimensional Dynamic Consent (MDDC) model are effectively enforced on Ethereum to

manage access control over sensitive data. These attributes align closely with the privacy and security requirements of Smart Home Healthcare Ecosystems (SHHE), significantly enhancing user trust and system integrity through verifiable and tamper-resistant records of data access interactions.

3.4.2.1 Scenario of Privacy Score Computation

Scenario 1:

A smart home healthcare system handles requests for three types of data i.e., medical history, lifestyle data, and environmental data, from three roles: a doctor, a family member, and a researcher. The data includes records from various periods.

(i) Static Privacy Score Computation:

1. Input Data:
    - Role-Based Weight (ωr): Refer to Table 3.2.
    - Data Sensitivity Factor (γd): Refer to Table 3.2.
    - Time-Decay Factor (λ(t)):
        - Latest Data (0–30 days): λ(t) = 0.9
        - Recent Data (31–90 days): λ(t) = 0.7
        - Older Data (>90 days): λ(t) = 0.5
2. Calculations:
    - A doctor requests access to medical history recorded 45 days ago (λ(t) =0.7):

      $P_{static} = \lambda(t) \times \omega_r \times \gamma_d = 0.7 \times 0.9 \times 0.9 = 0.567$
    - A researcher requests the same data:

      $P_{static} = 0.7 \times 0.5 \times 0.9 = 0.315$
3. Threshold-Based Access:
    - Doctor: Moderate restriction ($0.4 \leq P < 0.7$).
    - Researcher: Low restriction ($P < 0.4$).

(ii) Dynamic Privacy Score Computation:

1. Historical Adjustments:
    - For the doctor (5 approvals, 1 denial):
        - $P_{dynamic} = \frac{1}{1 + e^{-\alpha(0.567 + \sum_{t=0}^{T}(allow_t - deny_t))}}$
        - Result: Adjusted score (P = 0.617)
    - For the researcher (3 denials):

- $P_{dynamic} = \frac{1}{1 + e^{-\alpha(0.315 + \sum_{t=0}^{T}(allow_t - deny_t))}}$
- Result: Adjusted score (P = 0.285)

Dynamic Computation (Historical Adjustments) and Threshold-Based Decisions:

- Doctor (5 approvals, 1 denial): Adjusted $P_{dynamic}$ (Moderate restriction)
- Researcher (3 denials): Adjusted $P_{dynamic}$ (Access denied)

Although $P = 0.285$ generally indicates standard access for $P < 0.4$, repeated denial patterns trigger stricter adaptive risk-based access controls, aligning with practical security implementations.

This example illustrates the calculation of static and dynamic computations of privacy scores and threshold-based decisions, for integration into the proposed blockchain smart contract implementation. It demonstrates the practicality and robustness of the proposed privacy model in managing access control dynamically while adhering to user preferences and system requirements

Scenario 2:

To further illustrate how the DPSM adjusts access control decisions in real-world healthcare data-sharing scenarios, consider a case where different users request access to patient records of varying sensitivity levels. The system dynamically computes privacy scores based on user role, data type sensitivity, and past access decisions.

For this example, assume that two user roles: i.e., Healthcare Providers (HCPs) and Researchers (R), request access to two data categories:

1. Medical Data (high sensitivity)
2. Wellness Data (moderate sensitivity)

To compute privacy scores, the DPSM equation (4) is applied. To illustrate the dynamic privacy scoring computations described an example scenario with illustrative parameter values is provided in Table 3.4. These values demonstrate the practical computation of privacy scores for different roles (Healthcare Provider and Researcher) and varying data sensitivity categories (Medical and Wellness Data). The computed scores derived from these parameters

subsequently form the basis of the illustrative visualisation presented in Figure 3.6, highlighting the variations in access restrictions based on role and data sensitivity.

Table 3. 4: Parameter Values for Privacy Score Computation

Parameter	Healthcare Provider (HCP)	Researcher (R)
Time-decay factor (λ)	0.95	0.95
Role-based weight (ω_r)	0.8	0.5
Data sensitivity factor (γ_d)	0.9 (Medical Data) / 0.6 (Wellness Data)	0.9 (Medical Data) / 0.6 (Wellness Data)
$Allow_t$	20	10
$Deny_t$	2	8
Response rate control (α)	1.2	1.2
CTS*(T)	5	5

*CTS =Current Time Step

Why is T = 5 Important?

- The privacy score computation depends on time decay ($\lambda^{(T-t)}$), which adjusts the influence of past access decisions.
- Without T, it may be unclear how the exponential decay factor applies to older access decisions.
- Including T = 5 explicitly in the table ensures transparency and facilitates accurate interpretation of the DPSM model.

For this scenario, recent access decisions influence the score more, meaning the time-decay factor (λ) is 0.9 (reducing past decisions' influence). The response rate parameter α is 1.2, making the system moderately responsive to changes.

Privacy Score Computation and Interpretation:

Using the DPSM equation, privacy scores are computed for each case.

1. HCP requesting access to Medical Data $Privacy_{HCP\text{-}M}$

$$P_{HCP\text{-}M} = \frac{1}{1 + e^{-1.2(\sum_{t=0}^{T} 0.95^5 \times 0.8 \times 0.95 \times (20-2)}}$$

Final Computed Score: 0.92

Interpretation: A privacy score of *0.92* is high, indicates *restricted access*, meaning additional verification may be required. This could also mean *access is likely to be restricted or denied* unless explicitly authorised.

2. Researcher requesting access to Medical Data

$$P_{R\text{-}M} = \frac{1}{1 + e^{-1.2(\sum_{t=0}^{T} 0.9^{(T-t)}(0.6 \times 0.95)(allow_t - deny_t))}}$$

Final Computed Score: 0.76

Interpretation: A privacy score of *0.76* suggests access might be *permitted with justification.*

3. HCP requesting access to Wellness Data

$$P_{HCP\text{-}W} = \frac{1}{1 + e^{-1.2(\sum_{t=0}^{T} 0.9^{(T-t)}(0.7 \times 0.75)(allow_t - deny_t))}}$$

Final Computed Score: 0.85

Interpretation: A privacy score of *0.85* means access is *moderately restricted.*

4. Researcher requesting access to Wellness Data

$$P_{R\text{-}W} = \frac{1}{1 + e^{-1.2(\sum_{t=0}^{T} 0.9^{(T-t)}(0.5 \times 0.75)(allow_t - deny_t))}}$$

Final Computed Score: 0.64

Interpretation: A privacy score of *0.64* suggests access is likely granted with minimal restrictions.

Computed privacy scores highlight:

- HCP (Medical Data): (Highly restricted)
- Researcher (Medical Data): (Moderately restricted)
- HCP (Wellness Data): (Moderately restricted)
- Researcher (Wellness Data): (Low restriction)

These privacy scores reflect access levels based on role priority, data sensitivity, and historical access decisions. The computed privacy scores are visualised in Figure 3.6 and derived directly from privacy scores computed in Scenario 2, utilising predefined role-based weights, data sensitivity factors, and historical access decision parameters (Table 3.4). Each bar represents the final computed privacy score for a specific role-data type combination, clearly illustrating the dynamic privacy scoring model's effectiveness in differentiating access controls based on contextual variables. The analysis highlights how DPSM dynamically adapts privacy decisions based on contextual factors, ensuring an optimal balance between data privacy and accessibility.

This dynamic privacy scoring model robustly aligns privacy protection levels with user-defined preferences and evolving contextual requirements, effectively automating nuanced access control decisions.

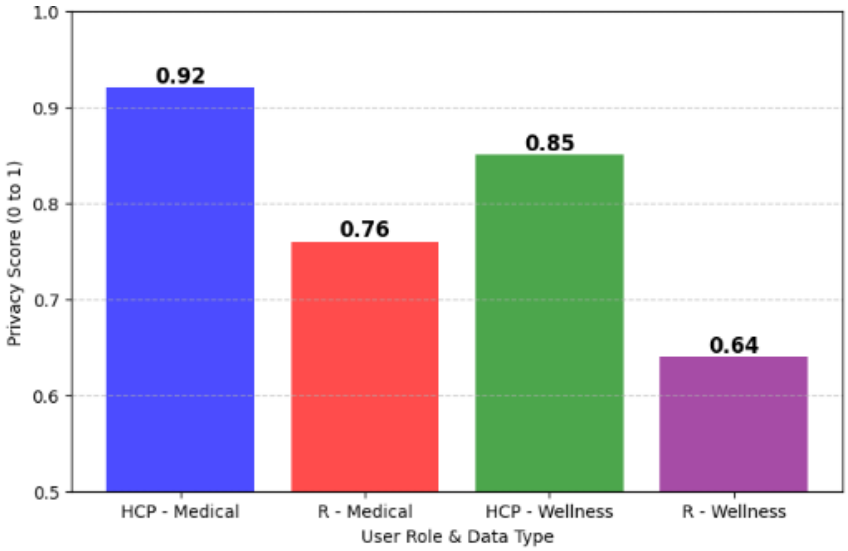


Figure 3. 6: Privacy Score Variation by Role and Data Type

In summary, DPSM computes access control decisions dynamically by integrating role-based weight (ω_r), data sensitivity (γd), and time-decay factors (λ). The computed privacy scores regulate access as follows:

1. Higher privacy scores (0.90 – 1.0) → Access Restricted or Denied (e.g., *sensitive medical data to unauthorised users*).
2. Moderate privacy scores (0.70 – 0.89) → Restricted Access Based on Context (e.g., *researchers accessing non-critical data*).
3. Lower privacy scores (0.50 – 0.69) → Access Permitted (e.g., *authorised personnel accessing general wellness data*).

This scenario demonstrates the effectiveness of DPSM in automating access decisions, enhancing privacy protection, and ensuring compliance with data governance policies. Notably, DPSM operates in an inverse relationship with an integrated Multi-Dimensional Dynamic Consent (MDDC) model, where higher privacy scores typically correlate with lower consent likelihood, and lower privacy enforcement enables greater consent flexibility. While DPSM establishes privacy boundaries, MDDC determines actual access permissions within those constraints, creating a context-aware authorsation framework. This relationship becomes

particularly important in scenarios requiring emergency overrides, where MDDC can adapt to urgent healthcare needs despite strict DPSM settings. A comprehensive examination of MDDC, addressing challenges such as consent fatigue and consent abuse, will be presented in Section 3.5 as part of evaluating the framework's resilience.

3.5 Model Validation and Refinement

The validation and refinement of the proposed privacy model are essential to ensuring its effectiveness, usability, and alignment with user expectations. This process adopted a comprehensive, iterative validation approach that combined quantitative analysis, qualitative feedback, and expert evaluations (Cawthra, et al., 2022; Nissenbaum, 2020). To achieve robust results, validation experiments were systematically executed over two instances of a 90-day testing period, using both real data collected from the testbed sensor setup (detailed in Table 3.1, Appendix D1) and simulated healthcare data interactions among network stakeholders within a Hardhat Ethereum blockchain environment. The better of the 90-day two instances was utilised for the performance evaluation. Detailed outcomes of these experiments are presented explicitly in Chapters 6 and 7."

To rigorously evaluate system performance and user interaction patterns, industry-standard analytics tools were employed, including Google Analytics for web application performance and Mixpanel for tracking detailed user interactions. Metrics such as navigation efficiency, task completion rates, and interface responsiveness were quantitatively assessed, complemented by qualitative feedback from survey analysis. Application reliability, error handling, and performance monitoring were further enhanced using New Relic, while user interaction patterns were visually analysed using heatmaps and session recordings via Hotjar.

3.5.1 Survey Methodology and Analysis

The survey methodology detailed in Chapter 6.3 was rigorous, clearly defining participant demographics, survey procedures, and consent handling. A total of 317 responses were initially collected, with a robust data-cleaning process reducing this to 300 valid responses. Exclusion criteria involved incomplete responses, inconsistent answers, duplicate submissions, and respondents lacking relevant experience in healthcare security management, ensuring a high-quality dataset reflective of real-world privacy concerns.

Participants (N=300) included healthcare providers, family members, researchers, and patients across varied age groups, genders, technological familiarity levels, health statuses, and geographic locations, providing robust demographic diversity. The structured survey questionnaire comprehensively covered demographic information, familiarity with smart home healthcare technologies and healthcare IoT, perceived benefits and drawbacks, data sharing preferences, privacy concerns, consent management, data sensitivity, transparency and control, trust in privacy-preserving technologies, and system acceptance of the privacy model. Consent handling was explicitly managed in accordance with GDPR guidelines, clearly informing participants about the nature of data collection, anonymity assurance, and the research purpose.

The survey analysis adopted a mixed-methods approach, using thematic analysis for qualitative feedback and statistical analyses (Chi-square tests, ANOVA, correlation analysis) for quantitative data. Additionally, usability testing employing the System Usability Scale (SUS) confirmed high levels of user acceptance and system usability, providing robust validation of the designed framework. From these 300 respondents, 56 participants interacted directly with the system via the intuitive dashboard and provided detailed feedback. Notably, within this subset, 19 participants were senior citizens (age 65 and above), offering essential insights into usability and acceptance among elderly users. User evaluation further involved observing participants' interactions with the intuitive frontend application, capturing real-life usability and acceptance insights. Expert evaluations by privacy experts, healthcare professionals, and ethicists complemented the user-based survey findings, ensuring robust validity and broad stakeholder relevance.

3.5.2 Threat Model and Attack Mitigation Strategy

The validation approach integrated comprehensive threat modeling, identifying specific attacker profiles, capabilities, and mitigation strategies within the smart home healthcare environment:

- **Attacker Profiles and Capabilities:** Identified attackers are categorised into three types and included External Adversaries (moderate technical skills, no system trust), Insider Threats (high capabilities, semi-trusted potentially honest-but-curious), and Smart Contract Exploiters (specialised technical knowledge, explicitly untrusted).

- **Attack Scenarios:** Critical scenarios such as poisoning attacks stemming from smart contract reentrancy vulnerabilities; consent abuse versus consent fatigue; Sybil attacks involving the creation of multiple fake identities to exploit privilege elevation (a form of man-in-the-middle (MITM) attack); and insider threats, for instance, authorised healthcare personnel attempting to bypass consent mechanisms using existing privileges, were systematically addressed and mitigated through blockchain immutability, efficient smart contract implementations, dynamic privacy scoring, anomaly detection, and consensus-based validation.
- **Trust Levels and Risk Assessment:** The trust model classified participants as Fully Trusted (data owners e.g. patients); Semi-Trusted a.k.a 'honest but curious' entities (e.g., healthcare providers who might act as honest-but-curious insiders - that might not behave according to protocol); Minimally Trusted (researchers, third parties); and Untrusted (external adversaries). Mitigation measures involved role-based access controls, dynamic privacy adjustments (DPSM), and multi-dimensional consent management (MDDC).

3.5.3 ML-Driven Optimisation

Machine learning-driven privacy optimisations were methodologically introduced and fully implemented in Chapter 7. Predictive privacy risk assessment leveraged machine learning techniques (Random Forest, Extra Trees classifiers), automating privacy-utility trade-off optimisation. This approach transitioned privacy enforcement from reactive to proactive, incorporating anomaly detection, adaptive privacy scoring, and risk-based adaptive access controls. The detailed validation of ML-driven mechanisms ensured accurate identification and mitigation of privacy threats, significantly enhancing system resilience and effectiveness.

3.5.4 Validation Techniques and Key Performance Indicators (KPIs)

The robustness of the validation framework involved extensive quantitative and qualitative analyses, specifically detailed in Chapters 6 and 7. Performance metrics included system scalability, smart contract efficiency, stress-testing outcomes, and data management effectiveness (IPFS storage integrity and upload/download times). User-related KPIs involved user satisfaction scores, frequency of privacy breaches, accuracy of access decisions, system responsiveness, and engagement levels with privacy settings. These indicators collectively

evaluated the overall system's effectiveness, user acceptance, and technical reliability. Additionally, user engagement with privacy settings was assessed to determine how effectively users interact with and customise their privacy preferences, providing insights into the system's accessibility and user-centric design.

3.5.5 Privacy Impact Assessment and Regulatory Compliance

Privacy Impact Assessments (PIA) and comprehensive compliance checks were integral parts of the validation methodology, ensuring adherence to GDPR, HIPAA, CCPA, and PIPEDA regulatory frameworks. Structured PIA approaches, coupled with threat modeling frameworks (LINDDUN and STRIDE), systematically evaluated privacy risks, informed iterative model refinements, and documented regulatory compliance. This inclusion and application of these established threat modeling frameworks such as LINDDUN and STRIDE was to uncover and address system-specific threats (Popoola O. , et al., 2023).

In practice, these methodologies provide a continuous process of monitoring and improvement throughout the system's lifecycle. Threat modeling identifies potential attack vectors, enabling the development of targeted mitigation strategies, while the PIA ensures alignment with user-centric privacy requirements and legal obligations. The findings from these assessments are documented to demonstrate regulatory compliance and serve as a foundation for iterative refinement of the privacy model. By adopting these practices, the methodology aligns with the overarching goals of creating a robust, adaptable, and secure framework for privacy-preserving mechanisms in smart home healthcare environments.

Table 3.5 provides a summary of the principles and safeguards of these regulatory frameworks, highlighting their focus on ensuring data protection and privacy across different jurisdictions and contexts.

Table 3. 5: Summary of the core principles across GDPR, PIPEDA, HIPAA, and CCPA

Principles	GDPR	PIPEDA	HIPAA	CCPA
Accountability	✓	✓	✓	
Lawfulness, Fairness, and Transparency	✓			✓
Purpose Limitation	✓	✓		
Data Minimization / Limiting Collection	✓	✓	Minimum Necessary Rule	✓
Accuracy	✓	✓		
Storage Limitation	✓	Limiting Use, Disclosure & Retention		
Integrity and Confidentiality / Safeguards	✓	✓	Security Rule	✓
Consent	✓	✓	✓	✓ (Explicit for data sale)
Openness / Transparency		✓		✓
Individual Access / Right to Access		✓		✓
Breach Notification			✓	✓
Enforcement / Penalties	✓	✓	✓	✓

Sources: (EUR-Lex, 2016; OPC, 2019; Edemekong, Annamaraju, & Haydel, 2018; ASPE, 1996; OAG, 2018).

3.5.6 Challenges and Mitigation Strategies

Validation also addressed specific implementation challenges, including balancing data utility and privacy, keeping pace with evolving regulations, diverse user needs, demographic limitations, sample biases, and potential privacy concerns or biases. Strategies included developing adaptive algorithms, establishing regulatory monitoring teams, conducting longitudinal studies, and complementing subjective self-reported data with objective behavioural analytics.

Table 3.6 illustrates these strategies which provided the foundation for addressing various technical and operational issues. These strategies were further validated and refined through user evaluation surveys, enabling the study to identify additional challenges and develop more comprehensive approaches based on real user feedback and experiences.

Table 3. 6: Challenges and Mitigation Strategies

Challenge	Mitigation Strategy
Balancing privacy with data utility for healthcare outcomes	Develop fine-tuned algorithms that maximise data protection while ensuring critical health information remains accessible when needed
Keeping pace with evolving privacy regulations	Establish a dedicated team to monitor regulatory changes and implement a modular system design for easier updates
Addressing diverse user needs and technical proficiencies	Implement adaptive interfaces and provide comprehensive user education resources
Sample bias (overrepresentation of tech-savvy participants)	Conduct additional targeted surveys or focus groups with less tech-savvy individuals; weight survey results to account for demographic disparities
Cross-sectional nature of the study	Implement longitudinal studies to track changes in user attitudes and behaviors over time; regularly update the model based on these long-term observations
Limitations of self-reported data	Complement self-reported data with objective measures (e.g., actual system usage data, behavioural analytics); use multi-method approaches to validate findings
Limited demographic scope	Expand future studies to include a broader range of age groups, socioeconomic backgrounds, and geographic locations; partner with diverse healthcare providers to reach a more representative sample
Potential social desirability bias in privacy concerns	Use indirect questioning techniques and scenario-based assessments to minimize social desirability bias; compare stated preferences with actual behavior in controlled experiments

In essence, the validation and refinement process detailed in this section and fully executed in Chapters 6 and 7 confirm the robustness, usability, and effectiveness of the proposed privacy model. This rigorous validation ensures that the framework is ethically sound, technically resilient, and closely aligned with user expectations, establishing a reliable foundation for the subsequent technical implementation detailed in Chapter 4.

3.6 Conclusion

This chapter presented a rigorous methodological foundation for developing a comprehensive privacy-aware authorisation framework within smart home healthcare environments. Adopting a longitudinal and iterative validation approach over a defined 90-day experimental tenure, the chapter outlined the integration of real-world sensor data and simulated blockchain interactions, ensuring the model's adaptability, robustness, and practical applicability.

The methodology systematically integrated ethical considerations, adaptive privacy scoring mechanisms (TDF, RBWF, DSF), dynamic consent management, and ML-driven optimisations, establishing a user-centric and context-aware privacy management framework. The structured mixed-methods approach, combining quantitative analysis (statistical evaluations, privacy score computations, SUS-based usability assessments) with qualitative user feedback (thematic analysis, expert reviews), ensured comprehensive model validation.

Detailed survey methodologies clearly outlined threat models, and explicit justifications for using Ethereum-based blockchain smart contracts reinforced the framework's validity and technical soundness. Additionally, comprehensive Privacy Impact Assessments (PIAs) and meticulous adherence to regulatory frameworks (GDPR, HIPAA, CCPA, PIPEDA) underscored its ethical rigor and compliance. The identified implementation challenges, coupled with proactive mitigation strategies, demonstrated thoughtful preparedness and adaptability to real-world constraints.

This robust methodological foundation now sets the stage for detailed technical realization and architectural implementation outlined in Chapter 4, confidently ensuring the designed framework meets both theoretical expectations and practical usability within smart healthcare applications.

Chapter 4

4. Design and Architecture of the Privacy-Aware Authorisation Framework

This chapter presents the technical design and architectural implementation of the proposed privacy-aware authorisation framework. Building on the methodological framework established in Chapter 3, it addresses critical challenges in managing healthcare data privacy within smart home environments, including data ownership, ethical disclosure, and user-centric controls.

The framework leverages advanced mathematical techniques to model dynamic privacy scoring and a multi-dimensional consent-based smart contract, integrated with blockchain technology to ensure scalability and adaptability. The design is centered on three key aspects:

1. ***Dynamic Privacy Scoring***: Adapting to user preferences and contextual changes.
2. ***Consent-Centric Authorisation***: Leveraging smart contracts for secure access control.
3. ***Intuitive User Interface***: Enabling granular privacy controls for end-users.

To explicitly illustrate how user-centric requirements have shaped specific design decisions, Table 4.1 presents an organised mapping of essential user needs to their corresponding architectural and technical solutions. This structured approach ensures transparency in how each requirement directly informs and guides the technical implementations described throughout this chapter, fostering a clear understanding of the rationale behind each design choice.

Table 4. 1: User Requirements and Corresponding System Design Specifications

User Requirements	System Design Specifications
Dynamic and context-sensitive privacy control	Implement dynamic privacy scoring with time decay and sensitivity.
Granular consent management	Multi-Dimensional Dynamic Consent (MDDC) smart contract framework.
Secure and transparent data sharing	Blockchain integration (Ethereum) and IPFS decentralised storage.
Compliance with regulatory standards	Auditable smart contract logs (GDPR, HIPAA compliant mechanisms).
Intuitive user interface	React-based dashboard for user-centric privacy management.

This chapter details the architectural components that underpin the framework, emphasising the interplay between technical design and ethical principles. It lays the groundwork for a robust and scalable system that supports secure data storage and user-centric privacy management.

4.1 Overall System Architecture

This section presents the architectural design of the proposed privacy-aware authorisation framework, detailing its components, interactions, and underlying mechanisms that enable secure data flow and privacy preservation in smart home healthcare environments. The architecture is designed to support dynamic privacy controls, secure data storage, and user-centric access management while ensuring scalability and interoperability.

4.1.1 High-Level Architecture Overview

The proposed system, the Privacy-Aware Smart Home Healthcare Ecosystem (P-ASSHE), is built on a multi-layered architecture to ensure secure data flow, privacy management, and scalability. This framework, illustrated in Figure 4.1, integrates privacy scoring and user-centric controls through a blockchain-based system to enable granular and adaptive data sharing.

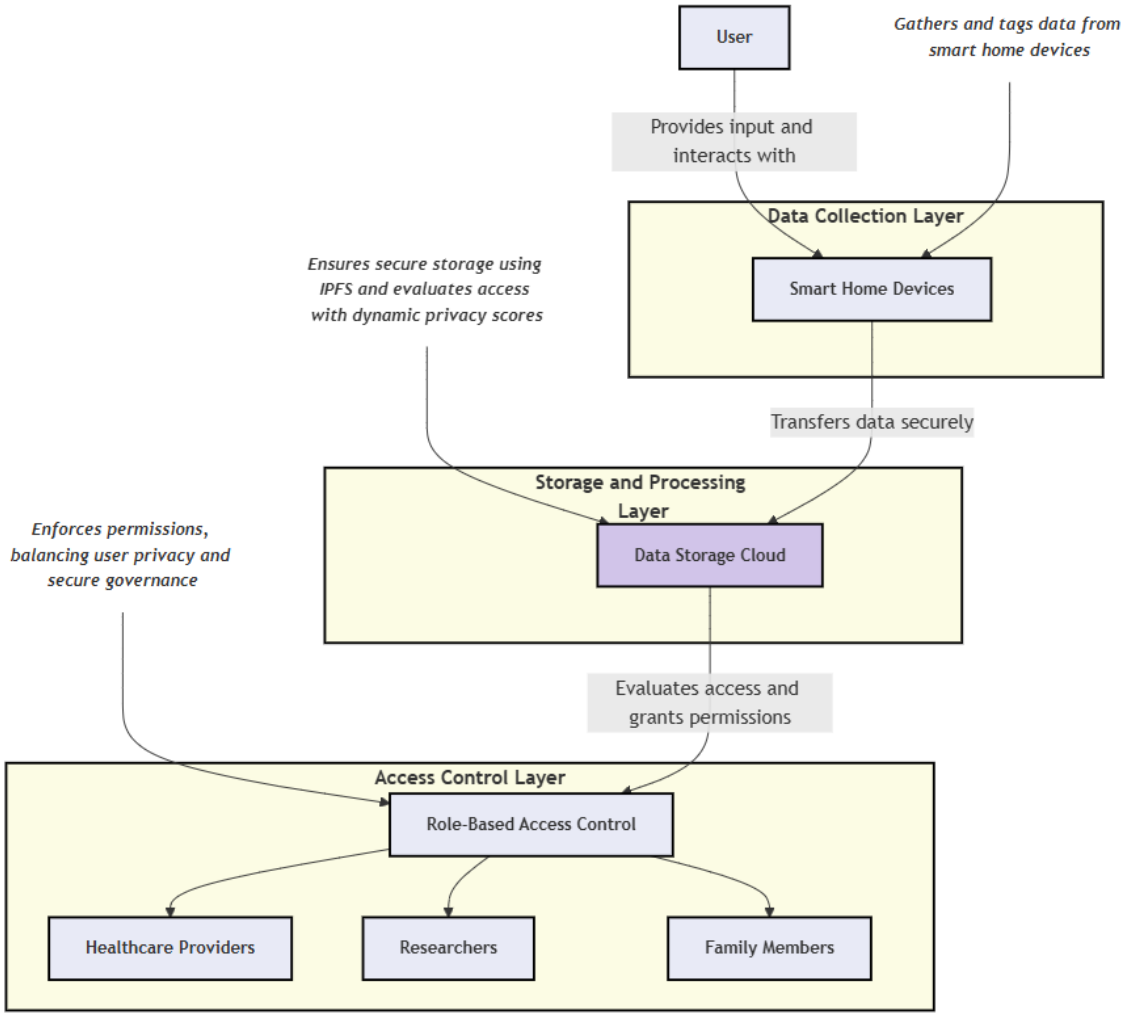


Figure 4. 1: High-level Architecture of the Privacy-Aware Authorisation Framework showing Access Control Mechanisms and Data Flow.

The architecture of this *HealthDataSharing* system comprises *Data Collection, Storage and Processing*, and *Access Control* layers. The *Data Collection Layer* gathers and tags data from smart home devices. The *Storage and Processing Layer* ensures secure storage using IPFS and evaluates access with a dynamic privacy score. The *Access Control Layer* enforces permissions for stakeholders, balancing user privacy and secure governance.

4.1.1.1 Actors and Functionalities in the HealthDataSharing System

The use case diagram (UCD) in Figure 3.3 (Chapter 3) illustrates the interactions between key actors and the proposed HealthDataSharing system within the Ethereum blockchain network configuration. The central actor in the system is the patient, who manages their health data and controls privacy settings. IoT devices are integrated to collect real-time health data for

monitoring purposes, while healthcare providers retrieve and analyse data for clinical decision-making. Research institutes focus on conducting anonymised data analysis for medical research, and family members receive notifications that support patient care.

Core system functionalities include data flow management, which represents the secure upload and storage of data on the blockchain. Access control mechanisms enable granting, revoking, and managing permissions to ensure secure data access, while privacy management tools empower users to define preferences for personalised data sharing. The blockchain integration is emphasised through the *Record Hash on Blockchain* feature, which facilitates interaction between the system and the Ethereum blockchain, and *Store in IPFS*, showcasing off-chain storage for efficient data handling. Security and encryption mechanisms are embedded within the framework, with *Encrypt and Decrypt Data* demonstrating the emphasis on secure data management across the system. These functionalities collectively enable a robust and privacy-centric healthcare ecosystem. Detailed UCD is presented in Appendix D.

4.1.1.2 Class Diagram Overview

The class diagram in Figure 3.4 (Chapter 3) illustrates the core components, blockchain integration, and stakeholder interactions within the HealthDataSharing system. At the core of the system are three main entities: the *Patient*, who manages data uploads, privacy preferences, and access permissions: *HealthData*, which securely stores encrypted health information in IPFS; and *AccessControl*, which governs permissions to ensure secure data sharing. The blockchain components, including *IPFSHash* and *BlockchainRecord*, facilitate integration with IPFS and Ethereum, ensuring secure storage of sensitive data. Additionally, *EncryptionDetails* provides cryptographic security for health information.

The system stakeholders, comprising healthcare providers, research institutes, and family members, interact with the system under defined roles and permissions, emphasising the modular design of the framework. Key functionalities include data flow modeling to capture interactions among patients, data storage, and stakeholders. Privacy and consent management capabilities enable granular control over data sharing, while analytics and research functionalities support privacy-preserving data analysis. Figure 3.4 (Chapter 3) underscores these interactions, showcasing a modular system architecture for privacy-aware data sharing.

4.1.2 Blockchain and IPFS Integration

This section discusses the integration of blockchain and the InterPlanetary File System (IPFS) to enable secure and decentralised healthcare data management. IPFS facilitates off-chain storage, addressing challenges of scalability, cost, and data integrity while ensuring efficient retrieval. By offloading large health records to IPFS, the framework reduces blockchain storage demands and costs. Content-based addressing ensures data integrity, while decentralised storage enhances resilience and availability. Additionally, version control in IPFS maintains access to historical records by preserving previous states of stored data, allowing retrieval of past versions when necessary.

Health data is encrypted using hybrid methods (ECC-256r1/AES-128/EAX) before IPFS upload. The resulting unique content identifier is linked to a smart contract on the Ethereum blockchain for secure access and retrieval. Figure 4.2 illustrates the data retrieval workflow, which involves authorised access requests, retrieval of the IPFS hash, and decryption for user access. This approach ensures robust, scalable, and secure data handling, complementing blockchain transparency and security. The integration of IPFS with blockchain ensures decentralised storage, where encrypted health data is stored off-chain while access control mechanisms are enforced through smart contracts on the blockchain. This enhances scalability, security, and historical version tracking of healthcare records.

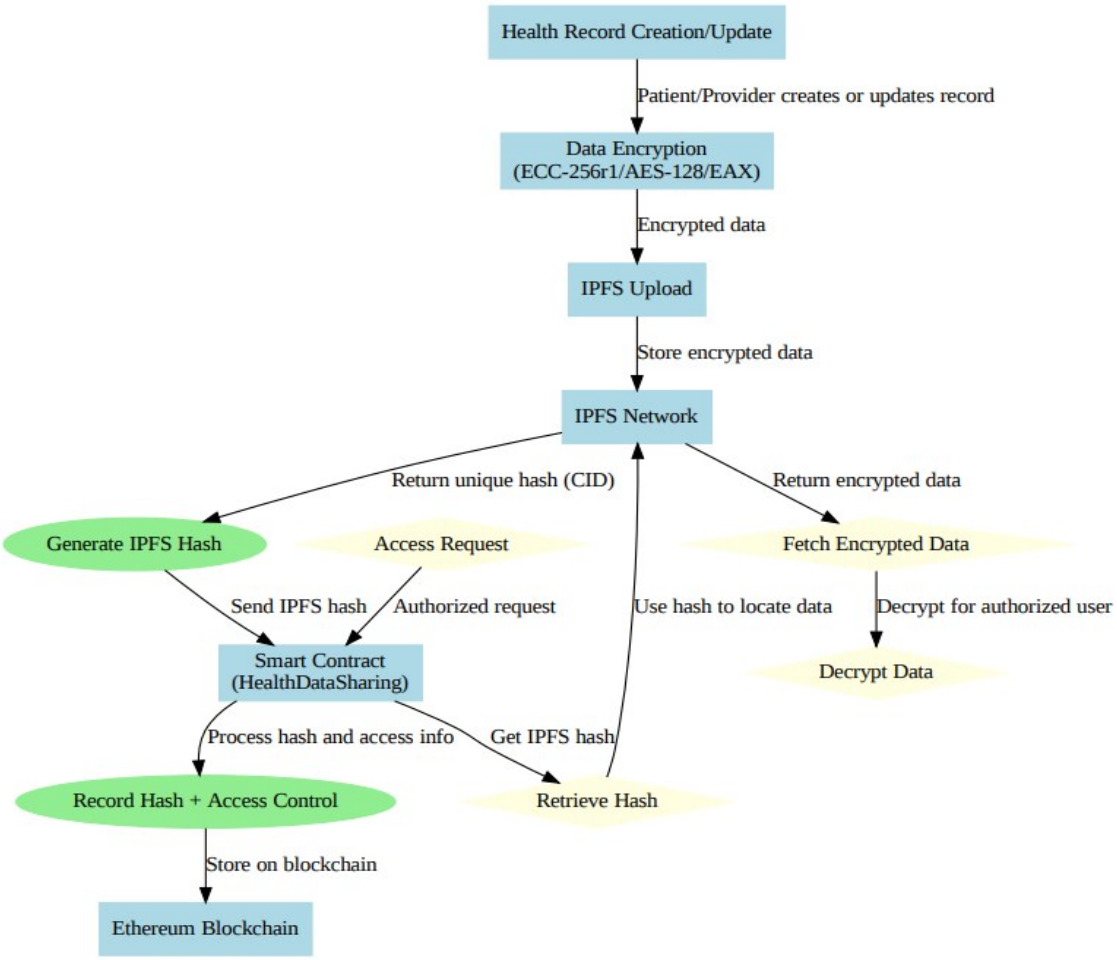


Figure 4. 2: IPFS Storage Flow

4.1.2.1 Ethereum Smart Contract Proposed Deployment Approach

This system employs Ethereum's smart contract capabilities to enforce privacy regulations and manage access control. The blockchain layer serves as an immutable permissions record, offering transparency and automated enforcement of privacy preferences. The proposed implementation integrates the following technologies:

- Solidity (Version 0.8.20) for developing smart contracts.
- Hardhat as the development and testing environment.
- Web3.js (Version 1.5.2) for blockchain interaction.
- MetaMask for transaction management and signing.

The design details of the proposed smart contract's foundational components, including variable initialisation, role-based authorisation, and data access functions, are available via the GitHub repository.

This deployment approach ensures secure data management, role-specific permissions, and seamless interaction with distributed storage systems like IPFS, offering a robust solution for privacy-aware healthcare systems.

4.1.2.2 IPFS for Decentralised Storage

The system leverages the InterPlanetary File System (IPFS) to achieve decentralised, secure, and scalable data storage, addressing privacy-preserving mechanism challenges like data ownership and integrity. Data security would be ensured through a hybrid encryption scheme that utilises ECC-256r1 for key exchange and AES-128 in EAX mode. The hashing algorithm adopted specifically for the IPFS storage implementation within this framework is SHA-512, selected due to its superior cryptographic strength and enhanced suitability for cloud-based storage solutions compared to the commonly employed SHA-256. The use of SHA-512 aligns seamlessly with the hybrid encryption scheme described here, ensuring robust security in hashing operations before data upload, thereby reinforcing the overall integrity of the data handling mechanism

The encryption and hashing operations occur before data is uploaded to IPFS, while smart contracts facilitate access control and reference management by handling the associated hash values, expressed as:

$$\text{Encrypted Data} = E_{AES}(D, K) \quad (5)$$

and

$$\text{IPFS Hash} = H(E_{AES}(D,K)) \quad (6)$$

where D represents the original data, K denotes the encryption key, and H signifies the hash function applied.

Encrypted data is uploaded to IPFS, generating a unique content identifier stored on the Ethereum blockchain. This links the data with access control policies while maintaining data integrity and minimising on-chain storage demands. The system ensures data ownership and integrity through the encryption of environmental and activity data before storage, storing only hash references on the blockchain, managing permissions via smart contracts, and empowering users through private key management. To improve data availability and persistence within the IPFS network, the system leverages the Pinata IPFS cloud service, for reliable pinning, ensuring that stored data remains accessible even in distributed environments.

The unique contribution of this research is explicitly showcased in Figures 4.3 and 4.4, which illustrate a novel approach to blockchain-IPFS integration architecture, distinctively featuring a blockchain layer as the primary orchestrator of access control through smart contracts. Unlike conventional blockchain-IPFS implementations, this framework uniquely integrates a dynamic privacy scoring model within Ethereum smart contracts to dynamically assess and facilitate access based on context-sensitive criteria. Specifically, the blockchain layer utilises smart contracts programmed with the Dynamic Privacy Scoring Model (DPSM) and the Multi-Dimensional Dynamic Consent (MDDC) model, enabling real-time computation of privacy scores and automated, adaptive consent management. This approach strengthens decentralisation while optimising retrieval efficiency and illustrate the integration workflow, detailing three key phases: (i) data collection from sensors and wearables based on user-defined privacy preferences, (ii) encryption and secure storage on IPFS with a corresponding hash stored on the blockchain, and (iii) the use of smart contracts for access control enforcement, privacy score computation, and dynamic access facilitation.

This integration ensures a robust, secure, and adaptive privacy management mechanism, directly embedding precise access-control logic within the immutable Ethereum blockchain. Such orchestration significantly enhances system transparency, data integrity, and user trust, reinforcing compliance with stringent regulatory standards such as GDPR and HIPAA. The detailed interaction workflow captured in Figures 4.3 and 4.4 highlights the hierarchical relationship between data collection from user-defined sensors and wearables, encryption and secure decentralised storage in IPFS, and dynamic access facilitation via smart contract-based controls. Further implementation details are presented in code design in the GitHub repository.

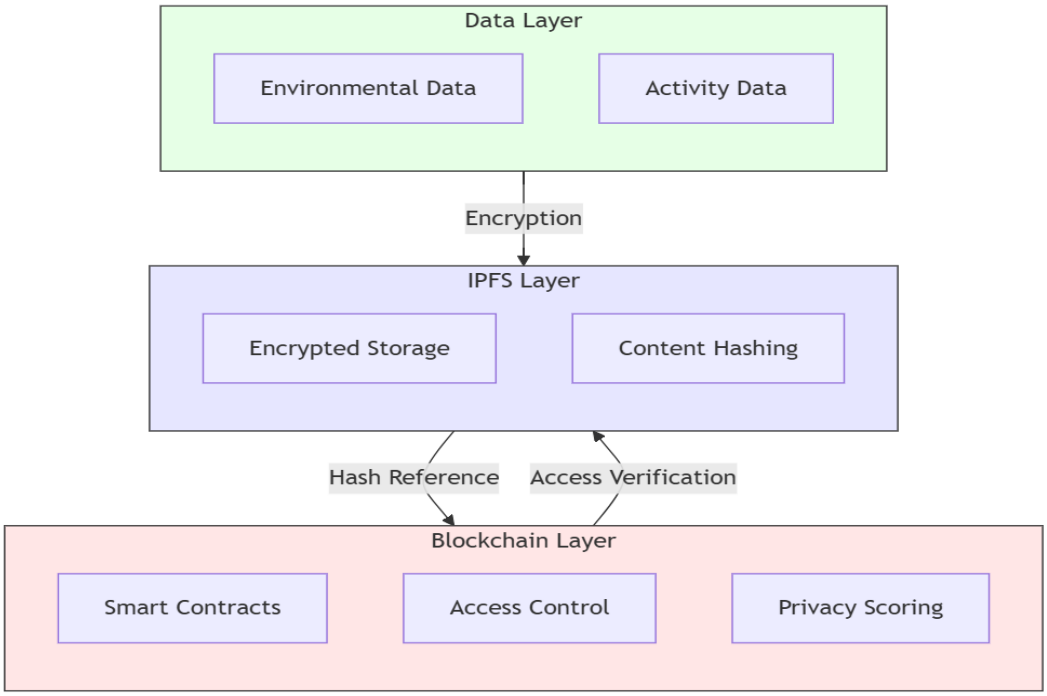


Figure 4. 3: Layered Architecture of the Blockchain-IPFS Integration showing the Hierarchical Relationship between Data, Storage, and Access Control Components.

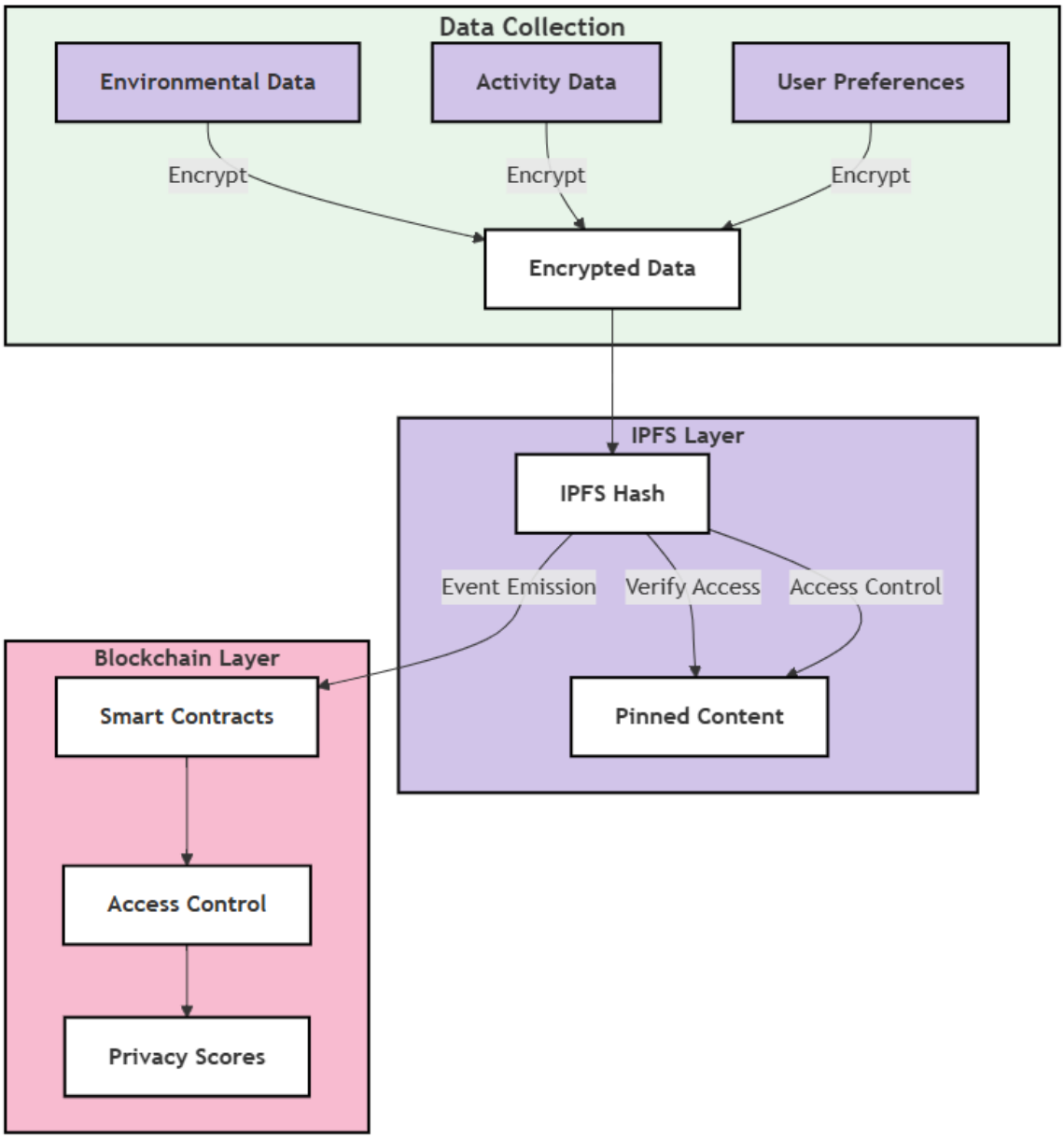


Figure 4. 4: Detailed data flow diagram illustrating interactions between components in the blockchain-IPFS integration, showing encryption, storage, and access control processes.

4.2 Privacy Control Components

This highlights the essential components of the core privacy-preserving mechanisms in the proposed framework. The *HealthDataSharing* smart contract serves as the backbone for core functionalities, including patient registration, health record management, access control, and consent logging. Figure 4.5 illustrates the integration of these components and their interaction within the system. The primary functionalities of the ***HealthDataSharing*** contract include:

- Managing patient registration and identity.
- Handling health records, including addition, updates, and retrieval.

- Implementing access control rules based on predefined roles.
- Logging and managing consent for data sharing.

Additional smart contracts support specialised tasks, such as token-based rewards for data sharing and dynamic consent management tailored to specific user needs, e.g., research participation incentives. These contracts interact seamlessly with the core contract, ensuring user autonomy and secure data sharing.

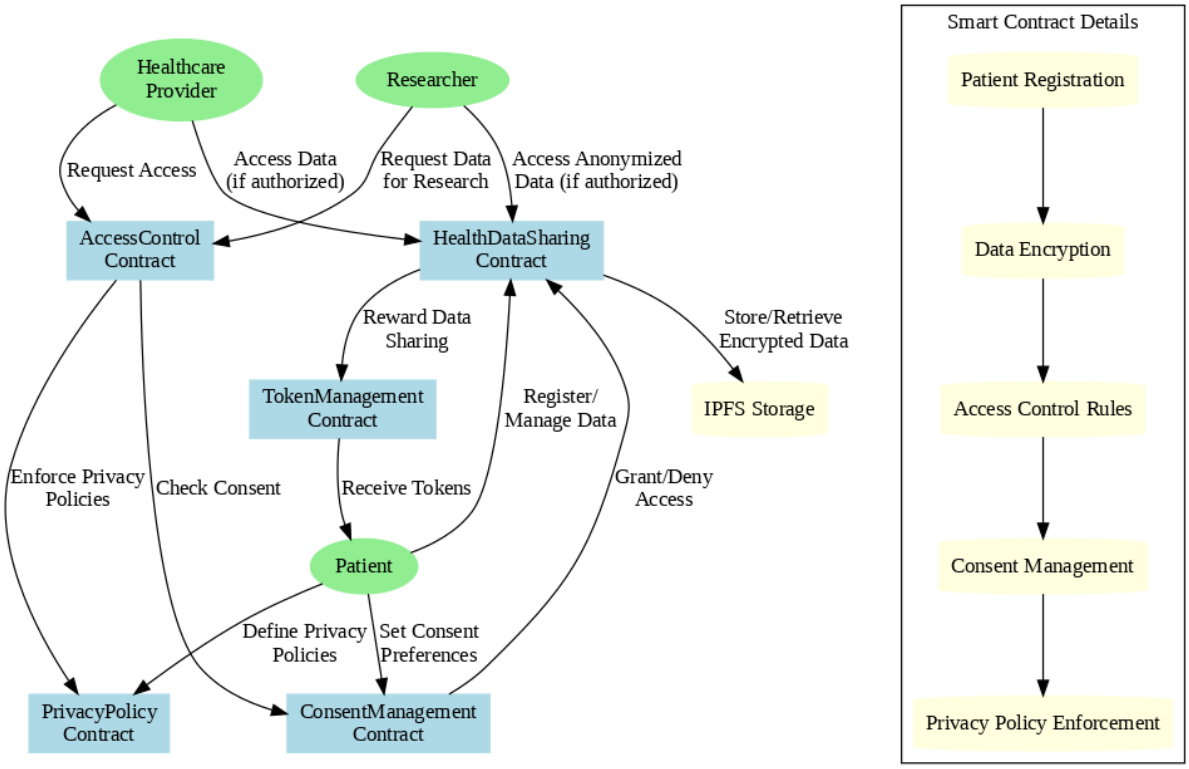


Figure 4. 5: Smart Contract Interaction

4.2.1 Dynamic Privacy Scoring Model

The dynamic privacy scoring model adapts to changing user preferences and contexts by quantifying privacy requirements through three key factors: time decay, role-based weights, and data sensitivity. This ensures appropriate protection levels for diverse data types. The privacy score P, for a user i at time n is calculated using equation (4) from Chapter 3:

$$P_n^{(i)} = \frac{1}{1 + e^{-\alpha(\Sigma_{t=0}^{T} \lambda^{T-t} \omega_r \gamma_d (allow_t - deny_t))}}$$

Where:

- $\lambda^{(T-t)}$: Time-decay factor, reducing the influence of older access events

- ω_r : Role-based weight (e.g., healthcare providers: 0.9, researchers: 0.5)
- γ_d : Data sensitivity factor (e.g., environmental data: 0.3, activity data: 0.6).
- α: Response rate control, determining the adaptability of the privacy score.
- allow_t and deny_t represent the cumulative number of allowed and denied access requests up to time *t*.

Figure 4.6 illustrates the computation process for producing a normalised privacy score ranging between 0 and 1, integrating key elements like time decay, role-based weights, and data sensitivity. This process operates across three hierarchical layers. The first layer, Input Factors (green), gathers primary influences on privacy. The second layer, Weight Values (purple), applies specific weights to roles and sensitivity levels, ensuring tailored computations. Finally, the Computation Layer (peach) combines these weighted values and normalises them through a sigmoid function. This structured approach ensures real-time adaptability to user behaviour, safeguarding privacy while facilitating authorised data access.

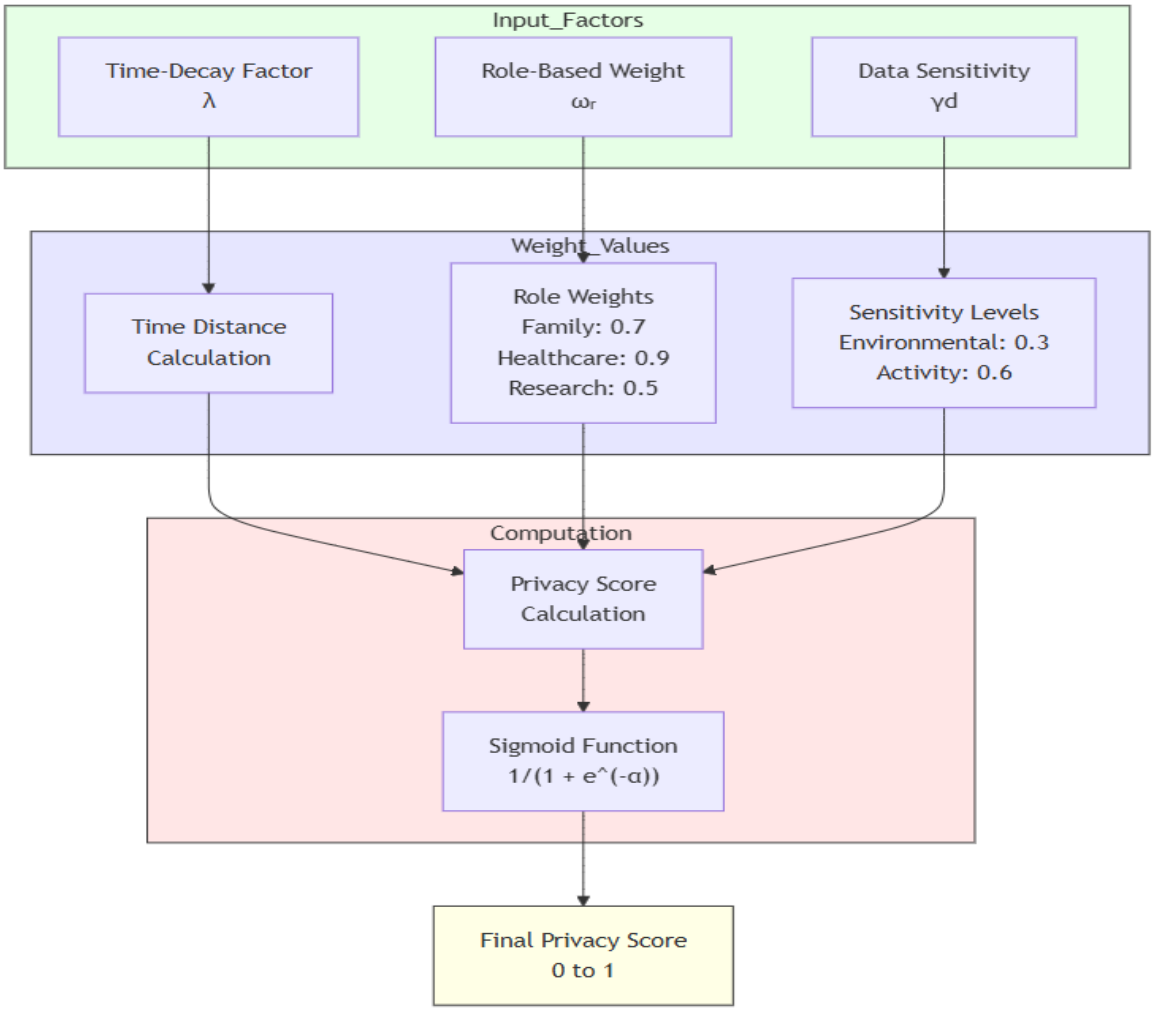


Figure 4. 6: Dynamic Privacy Score Computation Process showing the Integration of TDF (λ), RBWF (ω_r), and DSF(γd) for Privacy Score Calculation

4.2.2 Smart Contract Design

The *HealthDataSharing* smart contract is the foundation of the blockchain-based healthcare data management system, enabling secure data sharing, access control, and consent management while prioritising patient autonomy and privacy. Its hierarchical structure, depicted in Figure 4.7, comprises key components such as state variables, structs, events, and core functions.

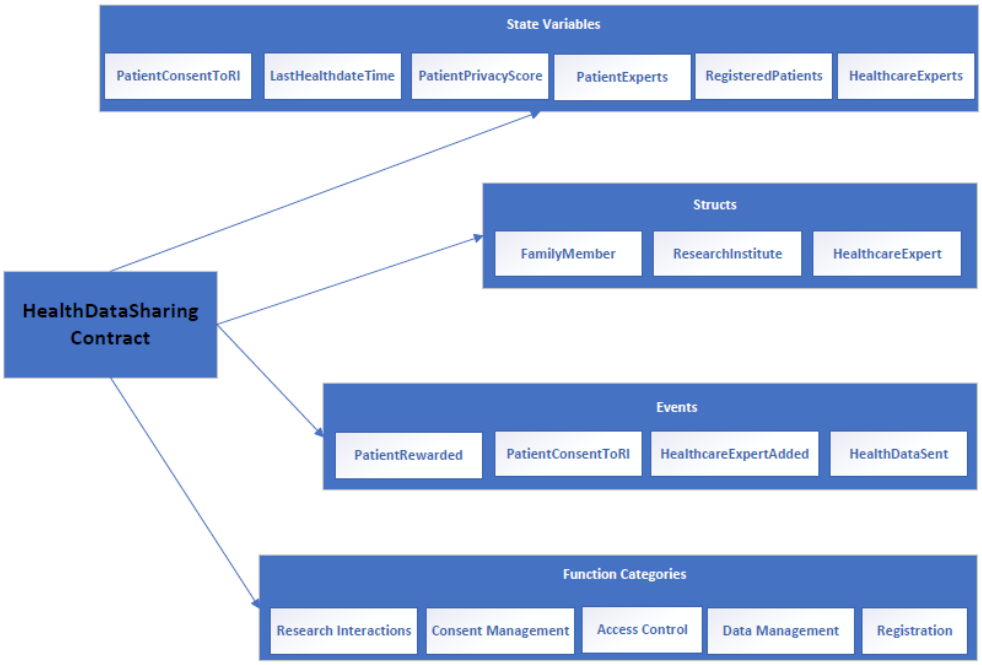


Figure 4. 7: Smart Contract Functional Architecture for Health Data Sharing

The contract incorporates key features to ensure secure healthcare data management. It supports patient registration and identity management, health record handling through IPFS integration, and granular access control with consent-based permissions. Patients can log and modify data-sharing preferences, while privacy-aware data-sharing ensures compliance with scoring mechanisms. Additionally, the framework enables anonymised research data sharing, balancing accessibility and stringent privacy requirements. This design grants patients control over their health information while supporting healthcare and research needs.

4.2.2.1 Contract Structure

The *HealthDataSharing* smart contract is organised around state variables, structs, and events to support secure data sharing and privacy controls.

- *State Variables*: Track patient registrations, healthcare experts, patient-healthcare expert authorisations, privacy scores, consent settings, and health data timestamps.
- *Structs*: Define entities such as healthcare experts, research institutes, and family members.
- *Events*: Emit logs for actions such as registration, authorisation changes, health data sharing, consent updates, and rewards.

This structure underpins the contract's ability to manage patient-centred healthcare data effectively.

4.2.2.2 Key Functions

The contract encompasses critical functions for managing patient registration, data sharing, and access control. It facilitates the registration of entities, such as patients, healthcare professionals, and research institutes, while allowing patients to define privacy preferences and manage consent through functions like `setPrivacyScore` and `setConsentToRI`. Secure data sharing is enabled alongside tools for notifications and access to time-based health data updates. Additionally, the contract supports research data sharing and incentivises patient participation through reward mechanisms.

4.2.2.3 Key Features Related to Data Ownership and Privacy

Emphasising patient autonomy and privacy, the design prioritises patient-centric controls that ensure all data-sharing actions require explicit initiation or consent. Granular access controls empower patients to manage permissions for individual healthcare experts, while privacy scoring dynamically adjusts access permissions based on consent preferences. The contract also incorporates audit trails to record significant actions, ensuring transparency, and role-based access controls to enforce distinct permissions for various users, such as patients, healthcare providers, and researchers.

4.2.2.4 Data Flow and Interaction Model

The smart contract structure shows the hierarchical organisation of components that enable secure data management and access control. Building upon these structural elements, the contract will implement specific data flow patterns to ensure secure and efficient data handling depicted in Figure 4.8. This illustrates the data flow within the system, showcasing how encrypted data moves through the contract's privacy control mechanisms to authorised access. The architecture integrates:

1. *Data Encryption and Storage*: Ensures secure storage using IPFS.
2. *Access Control Enforcement*: Regulates permissions based on privacy scores and roles.
3. *Event Emission*: Logs critical actions, supporting transparency and accountability.

This flow ensures efficient data handling from collection to authorised usage, maintaining security and privacy throughout the lifecycle.

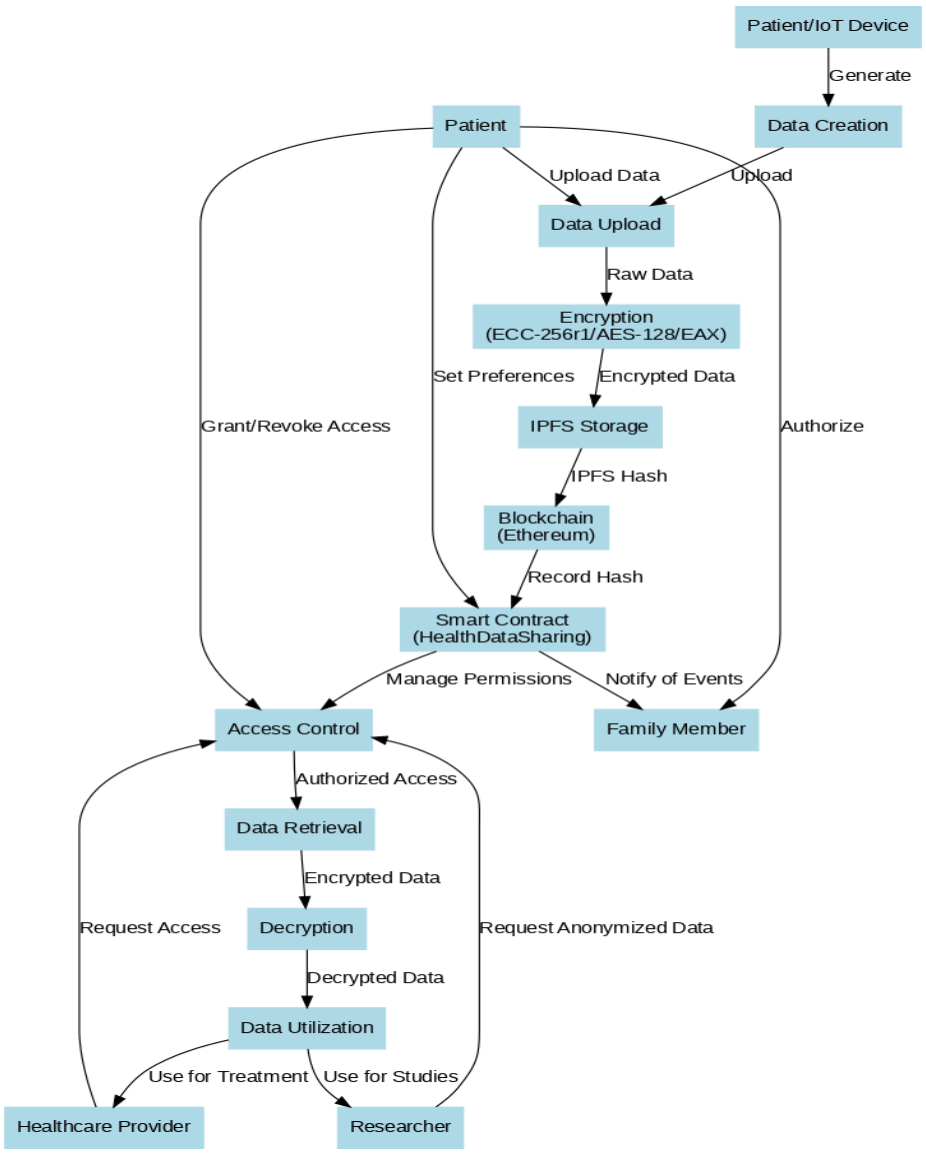


Figure 4. 8: Data Flow Architecture within the HealthDataSharing Contract

4.2.2.6 Contract Components Design

The Contract Components Design integrates essential features to ensure secure and efficient healthcare data sharing. Events for tracking healthcare data sharing and monitoring key metrics provide an auditable trail of actions within the system. Access control modifiers enforce role-based permissions, restricting unauthorised access to sensitive data. Additionally, core functions for patient and healthcare expert registration, including mechanisms to prevent duplicate registrations and enforce role-based permissions are included in the design of the

system. These components collectively ensure robust data management, transparency, and privacy. For complete design details, the codebase is available in the GitHub repository.

4.2.2.7 Privacy Controls Integration Design

The integration of privacy controls within the smart contract design ensures secure and privacy-aware data sharing. This integration leverages the privacy scoring system to enforce dynamic access control and validate user permissions. The design of role control and weight management, which forms the foundation of the privacy scoring mechanism, is detailed via the GitHub repository. To further ensure secure data exchange, the contract includes functions for health data transmission, timestamp tracking, and recipient notification is included in the code design.

The core privacy score access control functions, which manage data access permissions and validate privacy scores before granting access is presented in Appendix B1. These functions demonstrate how privacy scoring integrates with access control mechanisms within the MDDC framework. For instance, the checkAccessPermission function validates access requests based on a user's privacy score, ensuring that only authorised users can retrieve data. The getData function enforces this validation, dynamically adapting to the privacy preferences of system users. This is illustrated in Algorithm 4.1 showing the interplay between these core functions and the smart contract.

Algorithm 4.1 Privacy Score Access Control in MDDC Framework

Require: Requester address *requester*, Patient address *patient*
Ensure: Validated data access based on *privacy score*

```
function CheckAccessPermission(requester)
    if patientPrivacyScore[requester] ≤ 0 then
        Throw: "Privacy score not set"
    end if
    score ← patientPrivacyScore[requester]
    return ValidateAccess(requester, score)
end function
function GetData(patient)
    if CheckAccessPermission(msg.sender) is false then
        Throw: "Access denied based on privacy score"
    end if
    return RetrieveData(patient)
end function
```

Additionally, access control is enforced through modifiers like onlyRegisteredPatient, ensuring only registered users can interact with critical contract functions. Further interaction flow, detailed in Figure 4.9, highlights how stakeholders such as patients, healthcare experts, family members, and research institutes engage with the smart contract's core functionalities. These include role-based registration, access control, and privacy score management, collectively designed in the code base and available in the GitHub repository. This comprehensive design supports transparent audit trails, dynamic consent validation, and privacy-aware access control, ensuring secure and ethical healthcare data sharing.

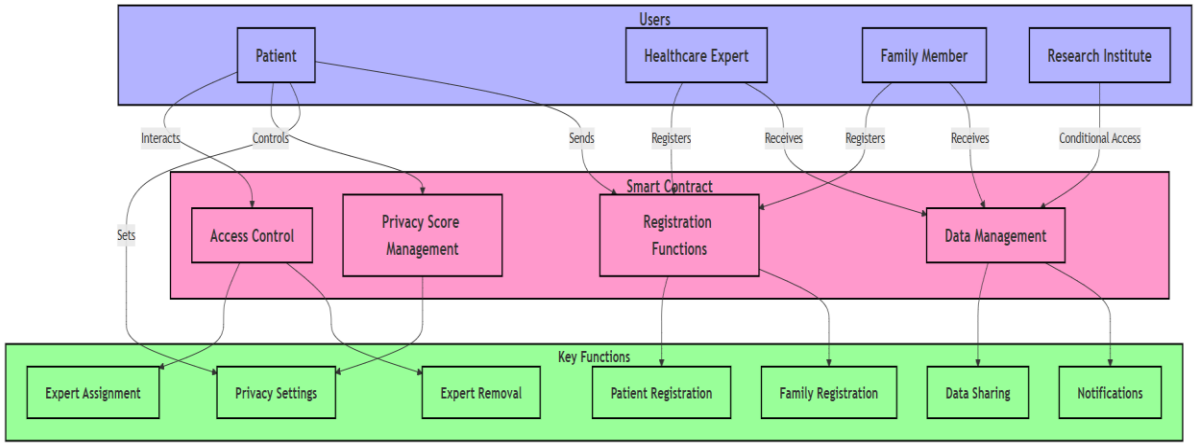


Figure 4. 9: Smart Contract Interaction Flow showing Relationships between System Users

4.2.3 Consent Management System

The consent management system implements user-centric control over health data sharing through a combination of smart contract functionality and intuitive interface controls. The system enforces explicit consent requirements, particularly for sharing data with research institutes, while maintaining transparency through event logging. This is represented by a smart contract indicating the basic consent management functionality i.e., (setConsentToRI and sendHealthDataToRI), and demonstrates the core validation checks and family member notifications. The design of the consent management for data sharing with research institutes ensures that patients' permissions are respected. This functionality, including consent setting and data-sending processes, is shown in Appendix B2 and can be accessed via the GitHub repository.

To enhance functionality and user experience, the system provides transparent consent tracking, ensuring real-time updates on consent status, emitting events for any consent changes,

and performing automatic validation before data sharing. Family member notifications are facilitated through automated alerts for data-sharing events, comprehensive activity logging, and role-based delivery of notifications. Furthermore, the system integrates a React-based consent management dashboard that provides real-time status updates and intuitive controls for managing consent effectively.

Figure 4.10 illustrates the consent management workflow, which shows the process of consent setting, validation, data sharing, and notification system within the smart contract implementation:

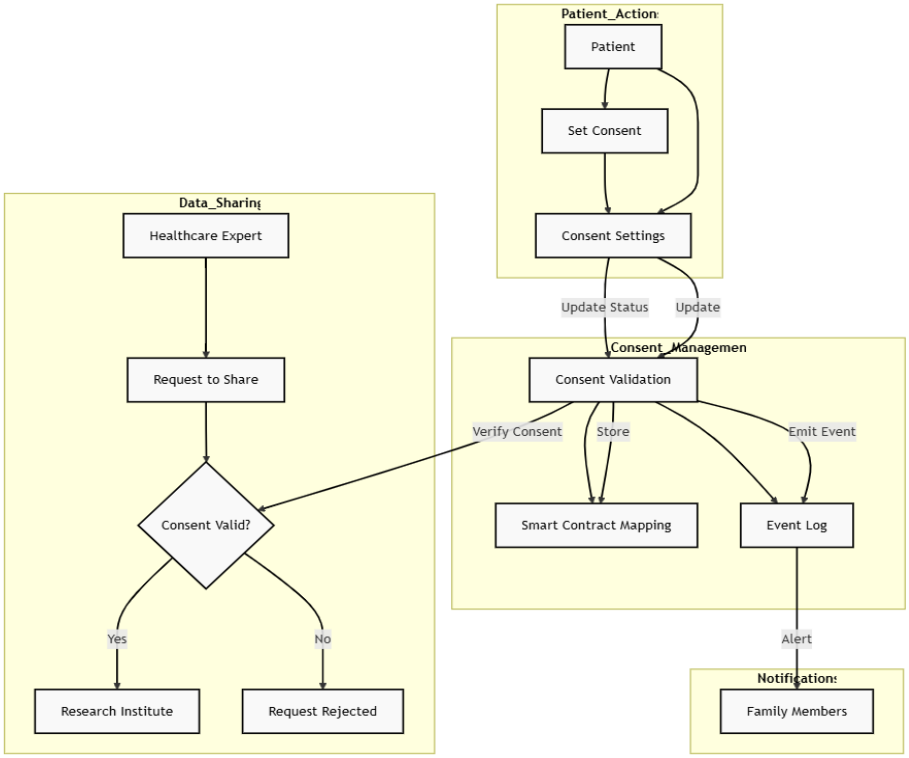


Figure 4. 10: Consent Management Workflow illustrating the Interaction between Patients, Healthcare Experts, and Research Institutes.

The consent management system builds upon the basic workflow shown in Figure 4.10 by implementing this novel Multi-Dimensional Dynamic Consent Model (MDDC). This enhancement transforms traditional binary consent into a context-aware, adaptive system that better reflects the complex requirements of smart home healthcare environments.

4.2.3.1 Conceptual Design of the Multi-Dimensional Dynamic Consent Model

To address the complex challenges of data ownership, privacy, and consent management in smart home healthcare environments, this study proposes a novel Multi-Dimensional Dynamic

Consent Model (MDDC). This model leverages the rich data available from IoT devices to create a nuanced, context-aware approach to data access and consent management. The MDDC introduces a comprehensive framework built on five fundamental dimensions that work together to create a contextually aware consent management system. Each dimension contributes to a holistic approach to privacy and consent management in smart home healthcare.

The Multi-Dimensional Dynamic Consent (MDDC) incorporates five core dimensions that collectively enable a robust and adaptive consent model. The *Data Type Classification Dimension* categorises data into three sensitivity levels: medical data, with the highest sensitivity (scored 9-10 on a 10-point scale), includes critical health metrics like heart rate and blood pressure; lifestyle data, such as step counts, calories burned, and sleep patterns, fall within medium sensitivity (6-8); while environmental data, including room temperature, humidity, and air quality, is classified as lower sensitivity (3-5). These classifications ensure appropriate granularity in data access permissions. The *Requestor Role Dimension* assigns varying levels of access based on the roles of the data requestor. For instance, primary care providers like doctors (Weight: 0.9) are granted full access to medical data and partial access to lifestyle and environmental data, while emergency services (Weight: 0.95) are allowed similar privileges due to their critical nature. Family members or caregivers (Weight: 0.7) are limited to lifestyle and environmental data with restricted access to medical information, whereas research institutions (Weight: 0.5) primarily access anonymised data, requiring additional consent for identifiable data.

The *Purpose of Use Dimension* evaluates the intended data use to determine access permissions, prioritising treatment as the highest purpose, and allowing unrestricted access to relevant data types. In contrast, care support limits access to lifestyle and environmental data, while research enforces controlled access through aggregated or anonymised datasets unless specific consent for identifiable data is obtained. The *Time Sensitivity Dimension* accounts for temporal factors such as real-time emergency access, scheduled care windows, and historical data access. The model enforces stricter access controls during nighttime and provides more flexible access during waking hours, with a time decay factor adjusting privacy scores dynamically to reflect temporal changes in consent sensitivity.

Lastly, the *Patient Context Dimension* ensures that the system adapts to the patient's real-time context, inferred from smart home data. For instance, current health status, such as sleep

patterns, may restrict data access when the patient is asleep except in emergencies. Location context and activity level allow broader access during periods of high activity, while environmental parameters and time-of-day considerations permit increased personal access if deviations from normal ranges are detected. These dimensions collectively enhance the flexibility, granularity, and responsiveness of the MDDC, creating a privacy-aware framework suitable for dynamic and user-centric consent management in healthcare settings.

The MDDC operates on a dynamic consent management system where patients can set baseline consent levels for each data type and role. These consent levels are then automatically adjusted based on the current context and privacy scores calculated using the previously described algorithm (Section 4.3.1). This approach ensures that data access remains aligned with patient preferences while adapting to real-time situations and evolving privacy needs. Figure 4.11 illustrates the interconnected dimensions of the MDDC, highlighting how each factor contributes to the overall consent and access decision-making process.

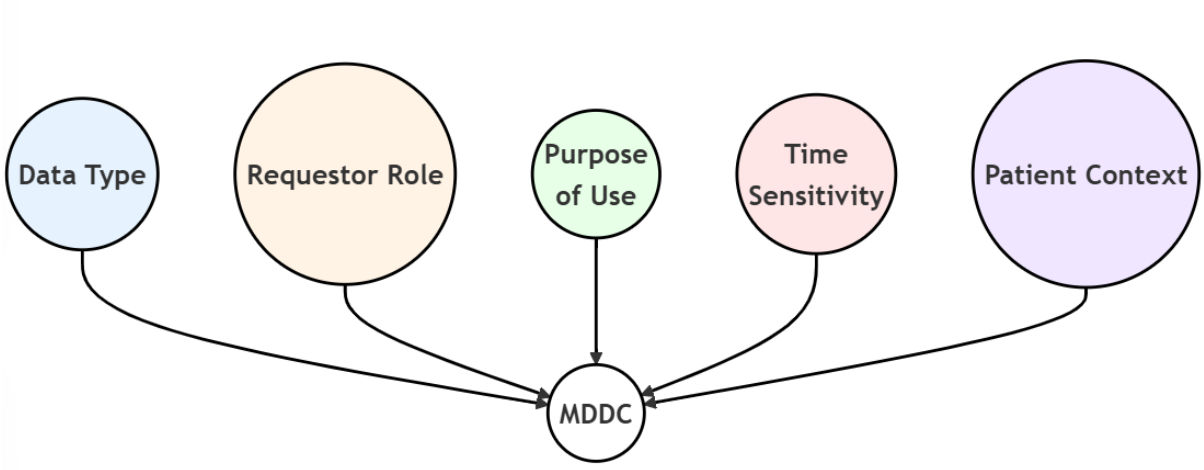


Figure 4. 11: Multi-Dimensional Dynamic Consent Model (MDDC)

By integrating these multiple dimensions, the MDDC provides a sophisticated yet flexible framework for managing consent and data access in smart home healthcare environments. This model significantly enhances data ownership and privacy protection while ensuring that necessary access for care and research purposes is maintained.

1. Mathematical Framework for the MDDC:

To formalise these dimensions into a quantifiable model, the Multi-Dimensional Dynamic Consent (MDDC) introduces a mathematical framework integrating all components into a unified scoring system. The MDDC score is computed using Equation (7):

$$\text{MDDC}_{score} = \alpha * \frac{\beta_1(DT) + \beta_2(RR) + \beta_3(PU) + \beta_4(TS) + \beta_5(PC)}{\Sigma \beta_i} \quad (7)$$

where *DT*, or Data Type Classification weight, captures the sensitivity of the accessed data with values ranging from 0.3 to 0.9, reflecting the heightened sensitivity of certain data types like medical records. *RR*, the Requestor Role weight, considers the role of the entity requesting access, such as healthcare providers or researchers, and ranges from 0.5 to 0.9, granting higher weights to entities with greater access authority. The Purpose of Use factor (*PU*) accounts for the intended use of the data, such as treatment or research, with a scale of 0.3 to 1.0, assigning higher values to essential purposes like medical treatment.

The framework also incorporates the Time Sensitivity coefficient (*TS*), which ranges from 0.1 to 1.0, to measure the urgency of access based on temporal contexts, such as real-time needs during emergencies. The Patient Context factor (*PC*) evaluates the patient's current state or preferences, with values from 0.2 to 1.0, to determine access permissions. An additional parameter, α, acts as an emergency override factor (Bhadoria et al., 2021), set to 1 for normal operations and 2 during emergencies to prioritise access. Finally, the weights *β1,β2,β3,β4, and β5* represent the relative importance of each dimension, summing to 1 ($\Sigma\beta i = 1$).

The MDDC mathematical framework integrates critical factors to ensure a robust and context-sensitive consent model. Figure 4.12 illustrates the computational workflow, detailing the systematic approach for translating contextual dimensions into the final MDDC score. The process begins with input factors derived from the five key dimensions: Data Type Classification (*DT*), Requestor Role (*RR*), Purpose of Use (*PU*), Time Sensitivity (*TS*), and Patient Context (*PC)*. These dimensions are assigned specific weights (β_1 to β_5), reflecting their relative importance, ensuring a balanced computation. Each dimension's weighted contribution is summed and normalised by the total weight ($\Sigma\beta_i$), resulting in an interpretable and bounded dynamic consent score.

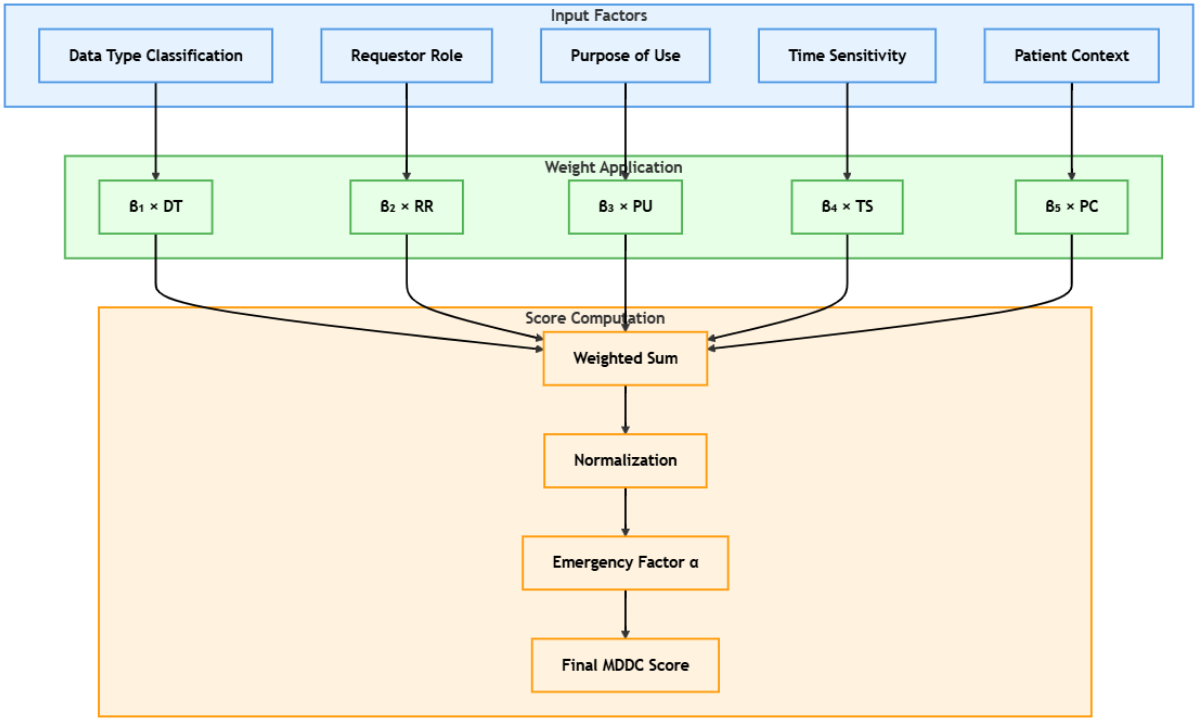


Figure 4. 12: MDDC Score Calculation Flow

The emergency override factor, α, provides adaptability during critical situations, prioritising access without compromising the integrity of the score computation. This flexibility ensures that the consent model can address both routine and exceptional scenarios effectively. Figure 4.12 demonstrates the practical implications of the mathematical model, offering sample visualisations of how varying factor combinations impact the resulting MDDC score.

The computational process highlights the model's modularity. Each step i.e., weight application, normalisation, and emergency adjustment, ensures that the consent decision remains transparent and systematically derived. The integration of these steps into a cohesive model supports the framework's objective of maintaining a balance between user preferences and operational exigencies. By leveraging the mathematical structure and visual representations, Figures 4.12 underscore the framework's robustness and applicability across diverse contexts.

Building upon the computational workflow, Figure 4.13 demonstrates the practical implementation of the MDDC scoring system through a comprehensive scenario-based calculator. This implementation directly translates the theoretical framework into tangible

outcomes, showing how the five key dimensions combine to produce meaningful consent scores across different healthcare contexts.

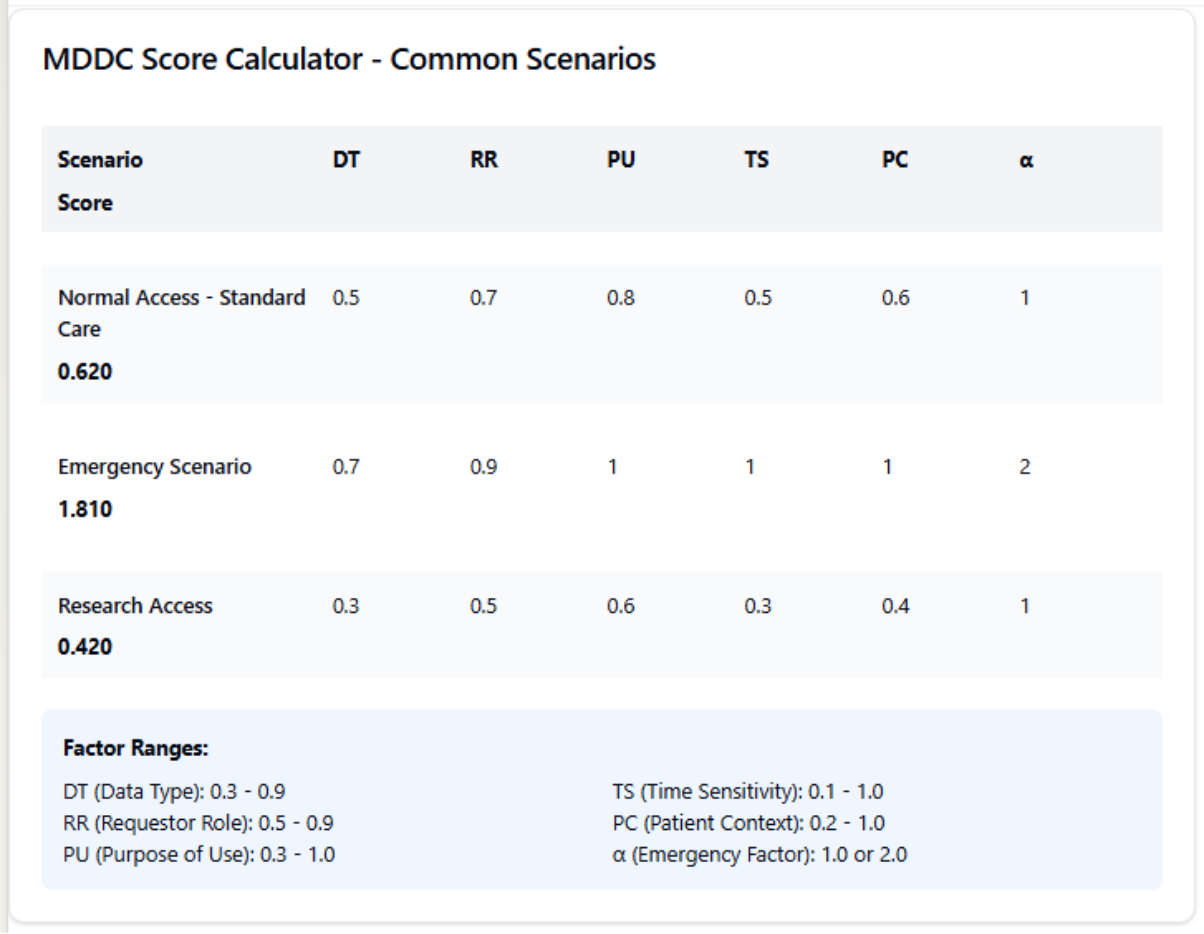
The calculator exemplifies three distinct scenarios that healthcare systems commonly encounter. In the standard care scenario, moderate values across all dimensions (DT=0.5, RR=0.7, PU=0.8, TS=0.5, PC=0.6) with $\alpha=1$ represent typical day-to-day healthcare operations. This baseline scenario produces a balanced MDDC score that reflects routine medical data access requirements while maintaining appropriate privacy safeguards.

Particularly noteworthy is the emergency scenario, where the mathematical framework's adaptability becomes evident. Here, elevated values across all dimensions (DT=0.7, RR=0.9, PU=1.0, TS=1.0, PC=1.0) combined with the emergency override factor ($\alpha=2$) demonstrate how the model responds to critical situations. The resulting higher MDDC score illustrates the framework's ability to prioritize urgent medical needs while maintaining a structured approach to consent.

In contrast, the research access scenario showcases lower values (DT=0.3, RR=0.5, PU=0.6, TS=0.3, PC=0.4) with $\alpha=1$, reflecting the less time-sensitive nature of research activities and their different privacy implications. This differentiation highlights the model's capability to appropriately adjust access permissions based on context-specific requirements. The relative weights (β_1 to β_5) remain constant across scenarios (0.25, 0.2, 0.2, 0.15, 0.2) to maintain consistency in the dimensional importance, while the varying input factors and emergency override multiplier (α) drive the context-specific adjustments. This approach ensures that while the basic structure of the consent model remains stable, it can still respond dynamically to different healthcare situations.

Through this practical demonstration, Figure 4.13 validates the theoretical framework earlier presented, showing how the mathematical model translates into actionable consent decisions. The calculator delivers both numerical outputs and valuable insights into factor combinations' influence on final consent determination, making abstract concepts more accessible to healthcare practitioners and system implementers. This implementation bridges the gap between theoretical design and practical application, demonstrating the MDDC framework's capability to provide nuanced, context-aware consent decisions while maintaining transparency and mathematical rigor. The clear presentation of factor ranges and their impacts helps

stakeholders understand and trust the consent determination process, facilitating its adoption in real-world healthcare settings.



MDDC Score Calculator - Common Scenarios

Scenario	DT	RR	PU	TS	PC	α	Score
Normal Access - Standard Care	0.5	0.7	0.8	0.5	0.6	1	**0.620**
Emergency Scenario	0.7	0.9	1	1	1	2	**1.810**
Research Access	0.3	0.5	0.6	0.3	0.4	1	**0.420**

Factor Ranges:

DT (Data Type): 0.3 - 0.9
RR (Requestor Role): 0.5 - 0.9
PU (Purpose of Use): 0.3 - 1.0
TS (Time Sensitivity): 0.1 - 1.0
PC (Patient Context): 0.2 - 1.0
α (Emergency Factor): 1.0 or 2.0

Figure 4. 13: MDDC Score Calculator for common healthcare scenarios.

2. Enhanced Mathematical Framework:

To enhance adaptability and ensure bounded consent scores, the MDDC model employs a sigmoid transformation, as expressed in Equation (8). This transformation ensures that the overall consent score, C(t), remains within a range of 0 to 1, providing an interpretable and scalable framework for privacy management. The equation integrates multiple weighted components, each corresponding to a critical dimension of the MDDC framework:

$$C(t) = \frac{1}{1 + e^{-\alpha(\sum_{d=1}^{D} \beta_d S_d(t) + \sum_{r=1}^{R} w_r R_r + \sum_{p=1}^{P} \gamma_d U_d + \lambda \cdot T(t) + \delta C_c)}} \quad (8)$$

Here, $S_d(t)$ represents the sensitivity score for data type d, such as medical, lifestyle, or environmental data, dynamically adjusting over time based on usage and context, with weights (β_d) ranging from 0.3 to 0.9, where higher values indicate more sensitive data. R_r denotes the

role-based weight for the requestor r, tailored to their authority level (e.g., healthcare providers, researchers, family members), with $\boldsymbol{\omega}_r$ values ranging from 0.5 to 0.9 (e.g., 0.9 for doctors, 0.5 for researchers). Similarly, U_p corresponds to the purpose-based weight for data usage p, such as treatment or research, with γ_p ranging from 0.3 to 1.0, higher for critical purposes like medical treatment. $T(t)$ accounts for temporal sensitivity, incorporating urgency or decay over time, with λ modulating time-based restrictions. C_c encapsulates patient context factors, considering elements like current health status, location, or environmental conditions, with δ values ranging from 0.2 to 1.0, where higher values signify greater contextual importance. Lastly, α enables emergency overrides by controlling the steepness of the sigmoid curve, with $\alpha = 2$ prioritising urgent access needs. The exponential form of the sigmoid function ensures smooth transitions between low and high consent probabilities based on the cumulative score of these dimensions.

Figure 4.14 visually depicts the integration process, highlighting how the MDDC model dynamically adjusts access permissions based on varying contextual factors. This systematic approach ensures that high-priority requests, such as those for medical emergencies, are granted prompt access while maintaining strict control over less critical data requests.

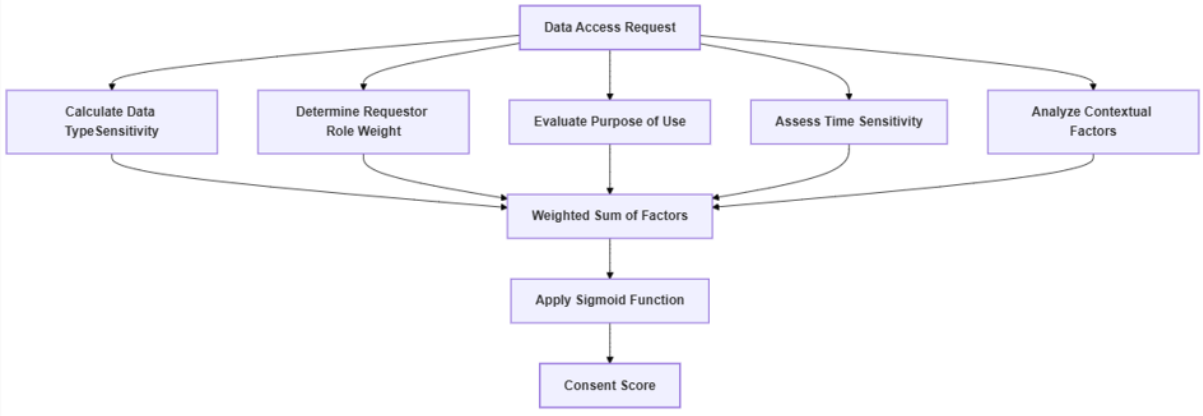


Figure 4. 14: Workflow of the MDDC Score Computation Process

To further interpret the practical implications, Figure 4.15 demonstrates the sigmoid curve's transformation of weighted sums into consent scores. For instance, a cumulative score of 3.81 results in a consent score of 0.98, indicating near-certain approval. This adaptability is vital in healthcare settings, where access decisions often require a balance between patient privacy and the urgency of data needs. The sigmoid transformation thus ensures that significant changes in

the input dimensions such as heightened data sensitivity or critical patient contexts are appropriately reflected in the computed consent score.

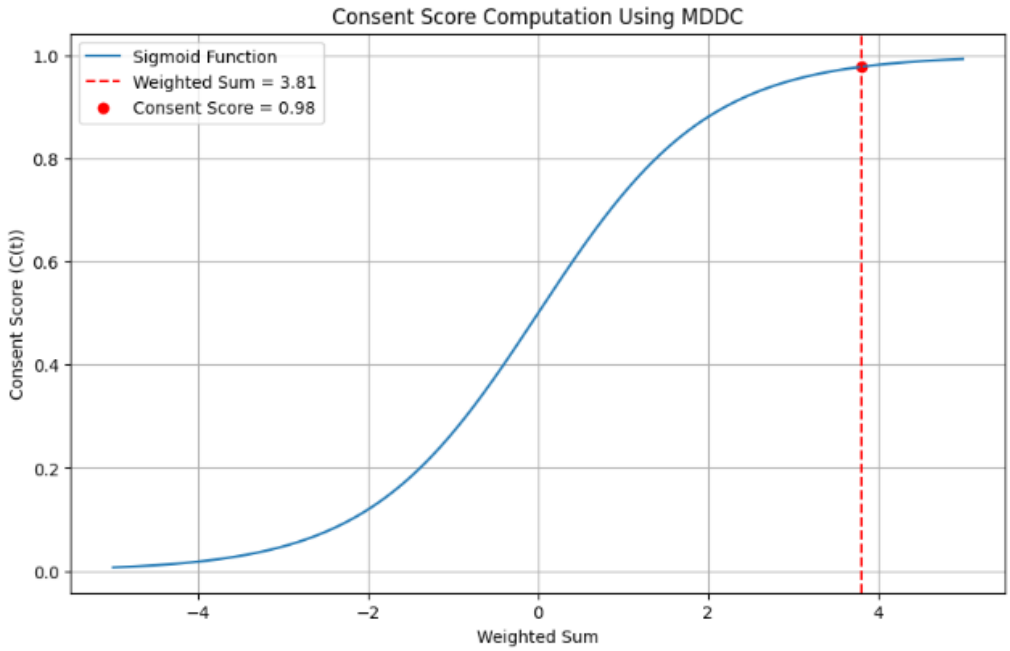


Figure 4. 15: Sigmoid transformation of the weighted sum into a bounded consent score, showcasing the dynamic adaptability of the MDDC model

By systematically addressing the dimensions of data sensitivity, requestor roles, usage purposes, temporal contexts, and patient-specific factors, the enhanced mathematical framework delivers a robust and interpretable approach to adaptive privacy management. This design supports dynamic adjustments to consent levels, aligning seamlessly with the requirements of modern, data-intensive healthcare environments.

4.2.3.2 Architectural Design of the Multi-Dimensional Dynamic Consent Model

The architectural design of the MDDC model advances traditional consent frameworks by integrating dynamic, context-aware privacy controls tailored for smart home healthcare environments. Central to this architecture is the incorporation of eight key features addressing data sensitivity, role-based access, temporal factors, and user context, all operating within a multi-layered smart contract structure. Figure 4.16 illustrates the overarching architecture, highlighting the interplay between these dimensions and the MDDC's adaptive functionalities. For instance, sensitivity scores, stored as smart contract variables, are dynamically adjusted based on data type and usage patterns, ensuring alignment with privacy

score calculations. The enhanced MDDC structures, as detailed in Appendix B3, establish the foundational data types and frameworks for managing sensitivity, roles, and contextual information, with the complete proposed design accessible in the GitHub repository.

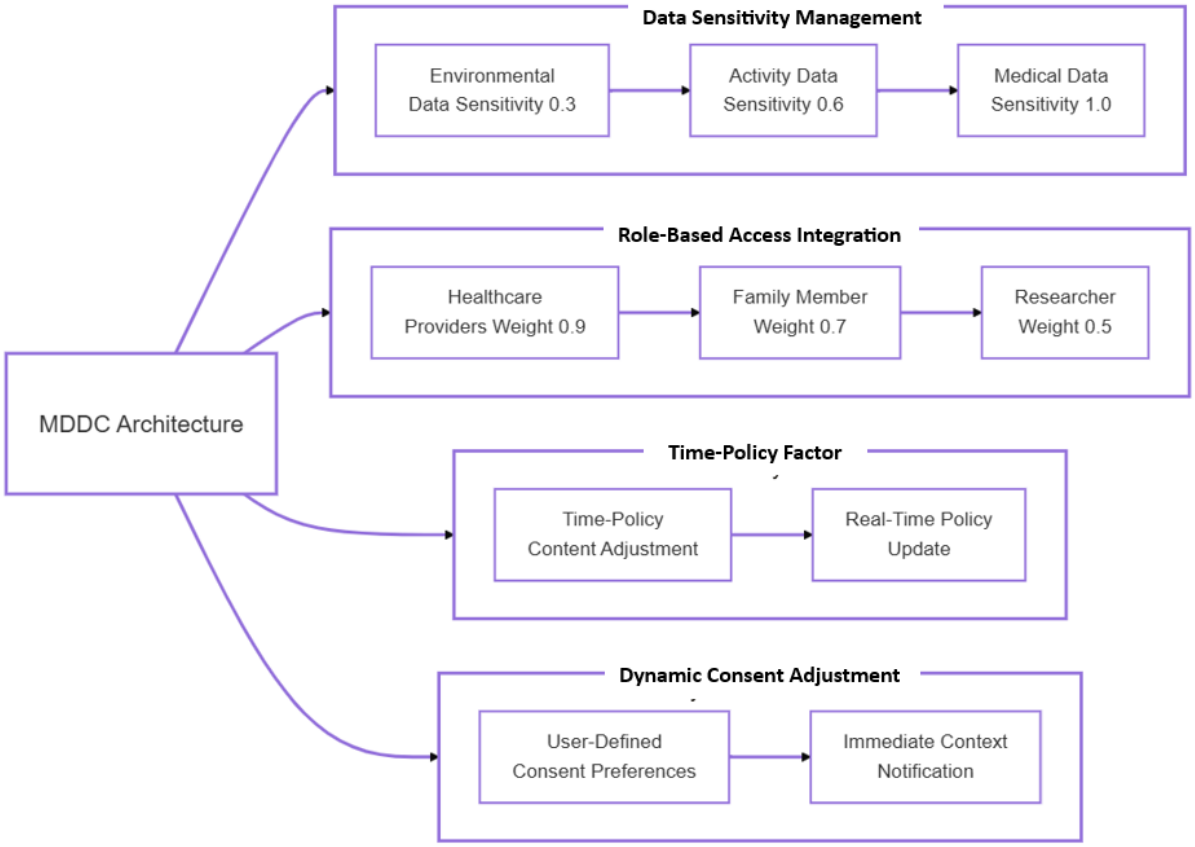


Figure 4. 16: Architecture of the MDDC

The system utilises state mappings and events to track consent relationships and ensure transparency. These mappings facilitate real-time updates to consent settings, supporting features like emergency access overrides while maintaining audit trails. Core consent functions, shown in Appendix B4 integrate the computational logic of consent scoring. By incorporating factors such as role weights, time decay, and sensitivity metrics, these functions ensure context-sensitive decision-making and adaptable access permissions. The design also introduces consent management functions, allowing users to modify preferences dynamically, revoke permissions, and enable automated updates in response to changing scenarios.

Dynamic role control mechanisms are a critical aspect of the system as shown in Appendix B5. These mechanisms ensure that access permissions are role-specific and adapt to real-time scenarios. For example, healthcare providers receive differentiated access to patient data based

on their roles and the sensitivity of the requested information. This role control is seamlessly integrated with the privacy scoring model to maintain a consistent approach to consent management across all system components.

The dynamic consent management module extends these functionalities by enabling users to modify consent dynamically, revoke permissions, and implement automated adjustments for evolving healthcare needs. This adaptability ensures that user privacy preferences are upheld without compromising data accessibility during critical scenarios. The dynamic consent management module dynamically adjusts access permissions using key contextual dimensions: *data sensitivity, role-based access control,* and *user-defined preferences*. Sensitivity values for medical records, well-being activity data, and environmental metrics are assigned and updated based on context, ensuring appropriate privacy controls. For example, medical records, due to their higher sensitivity (base: 0.9), enforce stricter access policies than environmental data (base: 0.3). These values, stored as smart contract variables, interact seamlessly with the dynamic scoring mechanism.

Role-specific weights further refine permissions, tailoring access to the needs of healthcare providers (weight: 0.9), family members (weight: 0.7), and researchers (weight: 0.5). For instance, healthcare providers are granted full access to sensitive health data, while researchers access anonymised data by default. The design implements this flexibility, enabling real-time adjustments to consent settings, such as granting or revoking permissions based on evolving scenarios like emergencies or routine healthcare updates.

This integration ensures fine-grained, context-aware control of health data sharing, prioritising user privacy preferences at every stage. The detailed logic behind role assignment and access controls ensures compliance with user-defined policies without compromising data availability during critical scenarios. The module's flexibility significantly enhances privacy-preserving mechanisms for dynamic healthcare environments.

Temporal and contextual dimensions play a pivotal role in ensuring adaptability. Time-decay factors prioritise recent consent settings, while emergency overrides allow immediate access when necessary, as illustrated in Figure 4.17. Contextual adjustments account for factors like patient location, status, and activity patterns, enabling the system to differentiate between routine and emergency data requests.

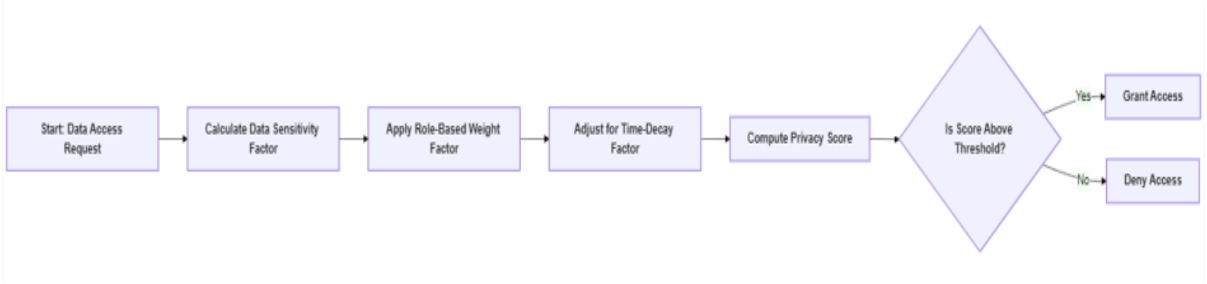


Figure 4. 17: Privacy score calculation workflow

Dynamic privacy scoring provides a unified, adaptable framework for managing role-based access rules, sensitivity settings, and time-decay factors. The Revocation Mechanism further strengthens the model's adaptability by enabling users to revoke permissions dynamically through a React-based interface. This ensures that unauthorised access is promptly curtailed, with the dashboard offering intuitive controls for managing consent, adjusting sensitivity settings, and modifying role-based permissions, as depicted in Figure 4.18.

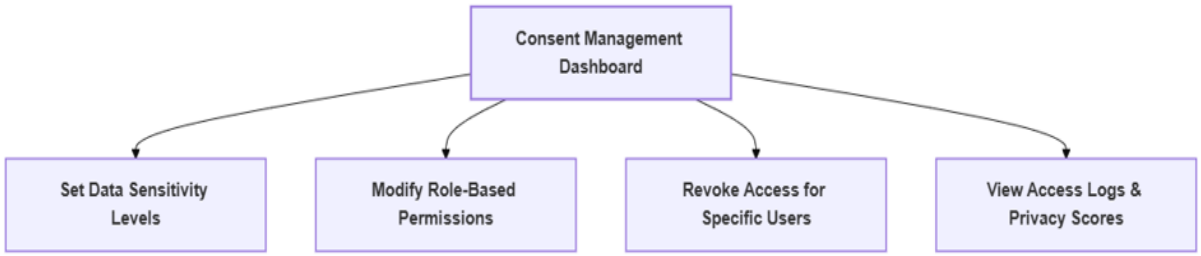


Figure 4. 18: MDDC User Interface Mockup showing Key Interactions.

Transparency and accountability within the system are bolstered by an *Audit Trail and Transparency* module. This module leverages the blockchain's immutable properties to create tamper-proof records of all interactions. To ensure robust cryptographic security, SHA-512 is specifically employed as the underlying hashing algorithm for audit trail management, aligning with the framework's approach to IPFS data storage hashing. By utilising SHA-512 to generate cryptographic representations of essential attributes including user identity, data identifiers, and timestamps, the framework achieves enhanced security assurances.

Equation (9) formalises the audit trail mechanism through a single cryptographic representation:

$$\text{Audit Entry} = \text{Hash}(\text{User ID} \parallel \text{Data ID} \parallel \text{Timestamp}) \quad (9)$$

This process ensures compliance with privacy governance standards while providing users with a robust mechanism for tracking data access events. Each input such as the user ID (representing the actor initiating an interaction), the data ID (indicating the resource accessed), and the timestamp (marking the exact time of the access) is concatenated and hashed to guarantee data integrity. These features enhances transparency and protect against unauthorised modifications, thus ensuring data ownership and privacy. Finally, the integration of dynamic consent workflows and privacy adaptation within the MDDC ecosystem ensures a seamless balance between privacy and data accessibility. By combining mechanisms like revocation, intuitive user interfaces, and audit trails, the proposed architectural framework empowers users while maintaining strict privacy compliance.

The MDDC components interact through a comprehensive flow that begins when a data access request is initiated from within the healthcare ecosystem, which could originate from healthcare providers, family members, or researchers. Upon receiving the request, the system performs a dynamic consent check based on the user's established preferences. The process then moves to a crucial calculation phase where the privacy score is determined by incorporating multiple factors including sensitivity levels, time decay considerations, and role-based weights.

Following the privacy score calculation, the system applies specific access rules based on the requester's role. A critical decision point then evaluates whether the calculated privacy score meets the required threshold for data access. Based on this evaluation, the system either grants or denies access to the requested data. In cases where access is granted, the system implements automated privacy adaptation based on recent interactions and updates consent preferences accordingly.

Throughout this process, every action, whether granting or denying access, is systematically recorded in an audit trail, ensuring complete transparency and accountability. This comprehensive interaction flow concludes once all necessary actions and recordings are completed. Figure 4.19 illustrates this interaction flow:

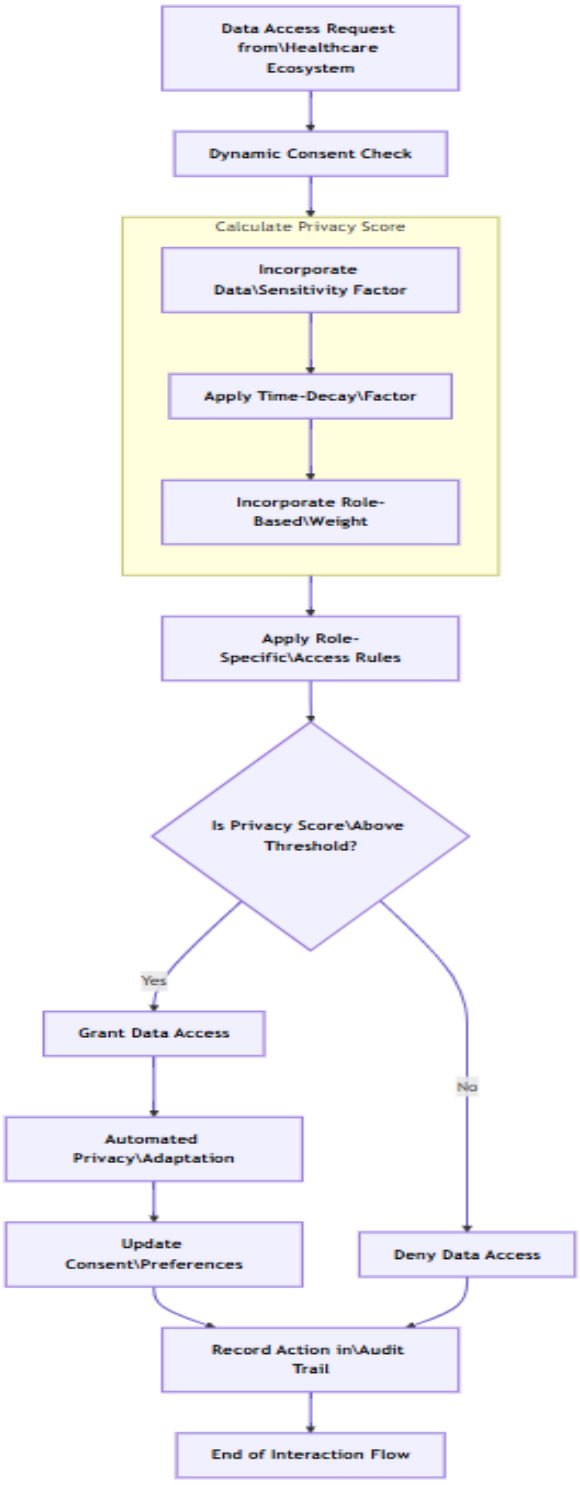


Figure 4. 19: Interaction flow of MDDC components

4.2.3.3 Illustrative Example for Equations 7 and 8

This subsection serves as an illustrative scenario demonstrating the consent score calculations using the Multi-Dimensional Dynamic Consent (MDDC) model. The parameter values shown in Table 4.1 are scenario-based, specifically designed for illustrative purposes, consistent with

the illustrative parameter tables used previously for privacy score computations in Table 3.4 (chapter 3)

Scenario Setup for MDDC Score Computation:-

To illustrate how the Multi-Dimensional Dynamic Consent Model (MDDC) computes consent scores, consider the following scenario:

A healthcare provider (HCP) and a researcher (R) request access to a patient's medical data and wellness data for different purposes. The patient's consent model dynamically adjusts based on five key factors:

- Data Type Classification (DT): Medical data has higher sensitivity than wellness data.
- Requestor Role (RR): Healthcare providers have greater access rights than researchers.
- Purpose of Use (PU): Treatment is prioritised over research.
- Time Sensitivity (TS): Emergency access is prioritised over routine requests.
- Patient Context (PC): The patient's real-time conditions affect consent decisions.

The MDDC Score for each request is calculated using Equation 7 in two complementary forms to enhance clarity and interpretability:

The first form explicitly outlines the individual dimension-specific contributions such as DT, RR, PU, TS, and PC, showing their linear combination and associated weights distinctly. This structured representation is ideal for explicitly demonstrating how each factor independently influences the Multi-Dimensional Dynamic Consent (MDDC) score.

1) $$\text{MDDC}_{score} = \alpha * \frac{\beta_1(DT) + \beta_2(RR) + \beta_3(PU) + \beta_4(TS) + \beta_5(PC)}{\sum \beta_i}$$

In contrast, the second form provides a concise summation (Σ notation) that encapsulates these individual contributions succinctly. This compact representation emphasises the cumulative effect of the dimensions, facilitating easier computation and practical implementation in computational frameworks or software systems. i.e.,

2) $$\sum_{i=1}^{5} \beta_1(DT_i \times RR_i \times PU_i \times TS_i \times PC_i)$$

Where in both cases:

- $\beta_1\, \beta_2\, \beta_3\, \beta_4 \beta_5$ are relative weights (sum to 1)
- α is an overriding factor (1 for normal requests, 2 for emergencies).
- DT, RR, PU, TS, and PC are dimension-specific values (ranging from 0 to 1).

Presenting both forms thus caters for preferences e.g., whether detailed explanatory insights or efficient computational usage, while maintaining mathematical consistency

To normalise the consent score, Equation 8 is applied:

$$C(t) = \frac{1}{1 + e^{-\alpha(\sum_{d=1}^{D} \beta_d S_d(t) + \sum_{r=1}^{R} w_r R_r + \sum_{p=1}^{P} \gamma_p U_p + \lambda \bullet T(t) + \delta C_c)}}$$

This ensures that the final consent score remains between 0 and 1, where higher scores indicate stricter consent requirements.

Using the scenario-based parameter values shown in Table 4.2 which are specifically designed for illustrative purposes, the computation of the MDDC score for different roles can be demonstrated.

Table 4. 2: Parameter Values Used for the Scenario

Parameter	Healthcare Provider (HCP)	Researcher (R)
Data Type (DT)	0.9 (Medical) / 0.7 (Wellness)	0.9 (Medical) / 0.7 (Wellness)
Requestor Role (RR)	0.9	0.5
Purpose of Use (PU)	1.0 (Treatment) / 0.7 (Wellness)	0.7 (Research) / 0.5 (Wellness)
Time Sensitivity (TS)	0.8 (Urgent) / 0.5 (Routine)	0.4 (Non-Urgent) / 0.3 (Routine)
Patient Context (PC)	0.9 (Critical) / 0.6 (Normal)	0.5 (General) / 0.4 (General)
Relative Weights (β)	0.25, 0.2, 0.2, 0.15, 0.2	0.25, 0.2, 0.2, 0.15, 0.2
Emergency Factor (α)	1.2 (Normal) / 2.0 (Emergency)	1.0 (Default)

Example 1: HCP Requesting Medical Data for Treatment (Urgent)

$MDDC_{HCP, Medical}$ = = 1.2× ((0.25×0.9×0.9×1.0×0.8×0.9) + (0.2×0.9×0.9×1.0×0.8×0.9) + (0.2×0.9×0.9×1.0×0.8×0.9) + (0.15×0.9×0.9×1.0×0.8×0.9) + (0.2×0.9×0.9×1.0×0.8×0.9))

=1.2×(0.1458+0.1166+0.0972+0.0648+0.0864)=1.2×0.5108 = 0.612

Using Equation 8, the normalised consent score:

$$C_{HCP, Medical} = \frac{1}{1+e^{-0.612}} = 0.648$$

Thus, the HCP receives a high consent score, requiring explicit patient approval.

Example 2: Researcher Requesting Medical Data for Research (Non-Urgent)

$MDDC_{R, Medical}$ = 1.0× ((0.25×0.9×0.5×0.7×0.4×0.5) + (0.2×0.9×0.5×0.7×0.4×0.5) + (0.2×0.9×0.5×0.7×0.4×0.5) + (0.15×0.9×0.5×0.7×0.4×0.5) + (0.2×0.9×0.5×0.7×0.4×0.5))

=1.0×(0.0315+0.0252+0.0189+0.0126+0.0158)=1.0×0.104=0.104

For examples 1 and 2, these expansions show the full calculation across all five dimensions with their respective weights (β values of 0.25, 0.2, 0.2, 0.15, and 0.2) applied to each parameter.

Using Equation 8, the normalised consent score

$$C_{R,\,Medical} = \frac{1}{1+e^{-0.104}} = 0.526$$

Thus, the researcher's request may require further authentication but is less restrictive than the healthcare provider's.

The outcomes of the illustrative scenarios are summarised and graphically represented in Table 4.3 and Figure 4.20.

Table 4. 3: The final consent scores for different access requests:

User Role & Purpose	MDDC Score	Normalised Score (C(t))
HCP - Medical (Urgent Treatment)	0.612	0.648
HCP - Wellness (Routine Check)	0.450	0.610
Researcher - Medical (Research)	0.104	0.526
Researcher - Wellness (Research)	0.080	0.520

The graphical representation of these results provides a clearer understanding of how different parameters affect consent scores as shown in Figure 4.20.

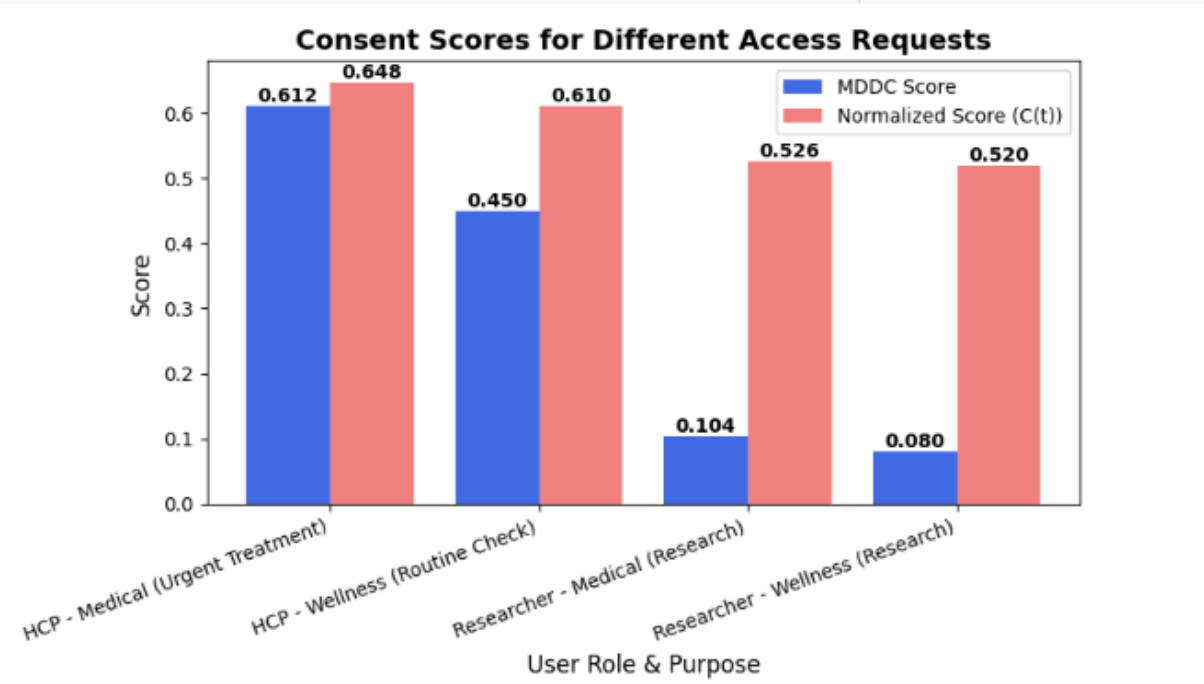


Figure 4. 20: Consent Scores for Different Access Requests

Conclusion: This illustrative example highlights how the MDDC model dynamically adjusts consent based on contextual parameters. Higher scores indicate stricter access control, ensuring that sensitive data remains protected while maintaining flexibility for authorised users. The inclusion of a graph and comparative analysis enhances the interpretability of these results.

4.3 System Requirements and Proposed Implementation

This section outlines the technical infrastructure, implementation requirements, and performance benchmarks for the proposed privacy-aware authorisation framework. It highlights the hardware and software specifications necessary to achieve secure and efficient data management, leveraging IoT devices, blockchain technology, and decentralised storage solutions. The following subsections discuss the technical requirements, system architecture, and integration components in detail, aligning with the framework's design principles to ensure privacy, scalability, and interoperability.

4.3.1 Technical Requirements

The privacy-aware authorisation framework is built on a robust technical foundation combining IoT sensors, blockchain technology, and IPFS-based storage. Key requirements address security, performance, and interoperability to meet the demands of a privacy-centric, user-friendly healthcare data management system.

Security Standards ensure data confidentiality and integrity. Hybrid encryption (ECC-256 for key exchange and AES-128 for data encryption) safeguards sensitive data transmissions. Smart contract-based role-based access control mechanisms dynamically adjust permissions using the Multi-Dimensional Dynamic Consent (MDDC) model detailed in Section 4.3.3. Blockchain immutability further supports integrity by recording consent changes and access logs, while Ethereum-based authentication and MetaMask integration prevent unauthorised access. Additionally, a blockchain-stored tamper-proof audit trail enforces compliance with GDPR and HIPAA standards, providing transparency and accountability.

Performance Requirements focus on ensuring seamless user experiences under varying loads. The system is designed to support up to 15,000 simultaneous data access requests with sub-200 millisecond latency during normal operations, scaling to handle peak traffic efficiently.

Decentralised storage using IPFS offloads large data files, enabling the system to maintain high throughput and minimise delays.

Interoperability integrates multiple components into a cohesive framework. Smart contracts on the Ethereum blockchain manage critical access and consent data, while IPFS handles large datasets, such as medical records, linked via unique hashes. A React-based frontend interacts with the blockchain backend through Web3.js, facilitating intuitive privacy management for users. Compatibility with diverse IoT devices ensures smooth data collection from wearable sensors, environmental monitors, and medical instruments.

Figure 4.21 illustrates the system architecture, highlighting the integration of blockchain, IPFS, and IoT devices. The blockchain layer manages access and consent via smart contracts, while IPFS decentralises the storage of larger datasets. IoT devices collect real-time health and environmental data and interface seamlessly with the system through backend integration, which bridges the IoT, blockchain, and IPFS layers. The front end provides an intuitive user interface for managing privacy settings and data access permissions.

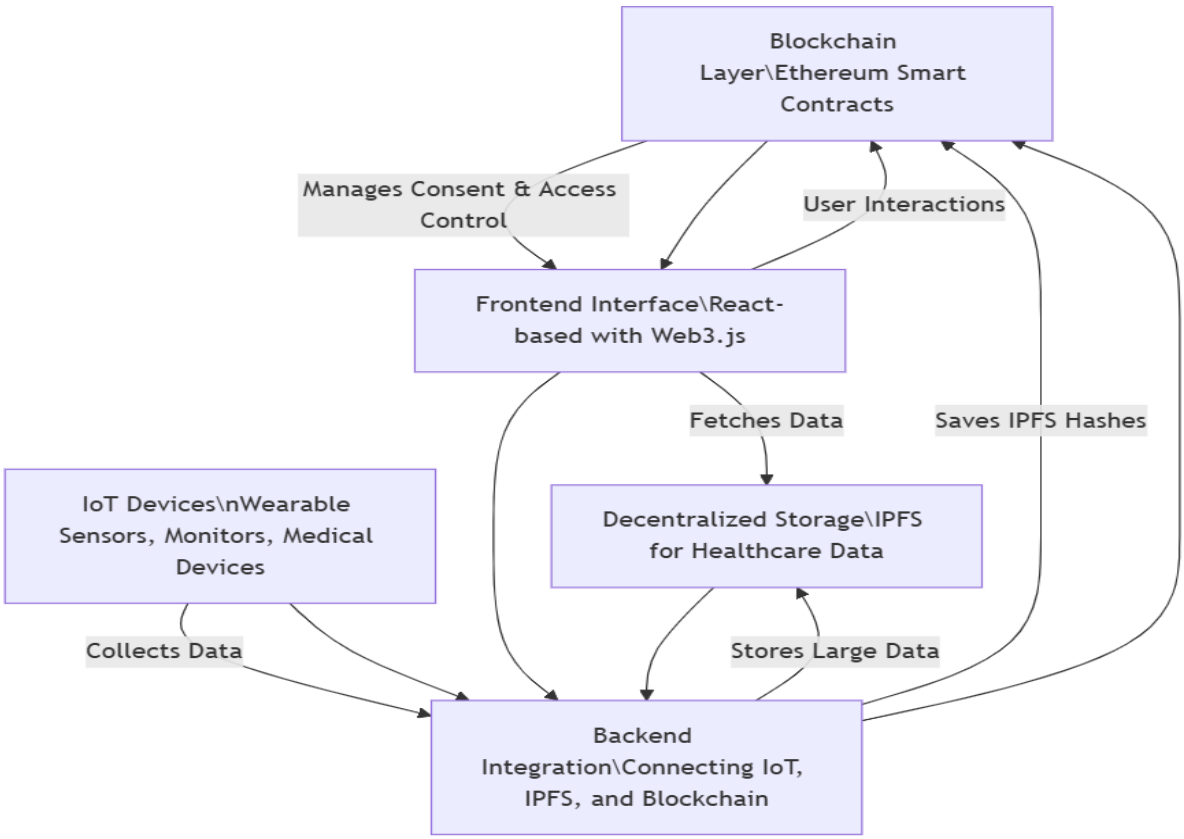


Figure 4. 21: System Architecture highlighting the Integration of Blockchain, IPFS, and IoT Devices.

4.3.2 Performance Metrics

To evaluate the framework's reliability and effectiveness, performance metrics aligned with healthcare standards and regulatory requirements were established. The target metrics are drawn from five authoritative sources:

(1) healthcare industry standards like HL7 FHIR guidelines for data exchange,

(2) data protection regulations such as GDPR and NHS Digital's DSP Toolkit,

(3) HIPAA technical safeguard requirements,

(4) benchmarks from blockchain healthcare implementations like MedRec, and

(5) international technical standards such as ISO/IEEE 11073 for healthcare communication and IEC 62304 for software.

Performance metric sources are detailed in Appendix B6.

These metrics fall into three categories:

1. **Transaction Processing:** The system targets 3,000-4,000 transactions per day, with a peak load capacity of 15,000 concurrent requests, ensuring a 99.5% transaction success

rate (Al-Turjman et al., 2020; Dang et al., 2019; Shen et al., 2020). These align with HIPAA availability standards and WHO surge capacity guidelines. The Hardhat development environment will simulate these conditions using IoT data sources.

2. **Storage and Data Integrity:** To meet HIPAA standards, IPFS operations aim for 99.5% data integrity. Uploads and retrievals target response times under 3 and 2 seconds, respectively, with 100% hash verification success to ensure consistency and accessibility under stress.

3. **Privacy and Security:** Privacy metrics aim for 0.90 score stability based on established privacy risk assessment frameworks in healthcare (Psychoula et al., 2020), maintaining consent update frequencies at 2-4 modifications per month. Authentication success is set at 99.5% enforcement accuracy, aligning with GDPR's explicit consent requirements and NIST cybersecurity standards.

Table 4.4 summarises the target benchmarks, illustrating alignment with established healthcare and security standards, ensuring robust compliance and reliability.

Table 4. 4: Benchmark Justification Summary

Metric Category	Target Value	Source/Justification
Transaction Processing	3,000-4,000/day	HL7 FHIR and Healthcare IoT Guidelines
System Stability	99.5%	HIPAA Requirements
Response Time	< 3 seconds	HL7 FHIR Performance Standards
Data Integrity	99.5%	HIPAA Security Rule
Privacy Score	0.90	NIST Cybersecurity Framework

Figure 4.22 illustrates these metrics, including transaction throughput, latency, scalability, and data integrity. Transaction throughput evaluates processing speed under peak loads, while latency assesses response times critical for real-time operations. Scalability measures the system's ability to handle growing demands, and data integrity ensures consistency and security, supporting trust in the framework. Privacy metrics monitor dynamic consent adjustments, ensuring alignment with user preferences.

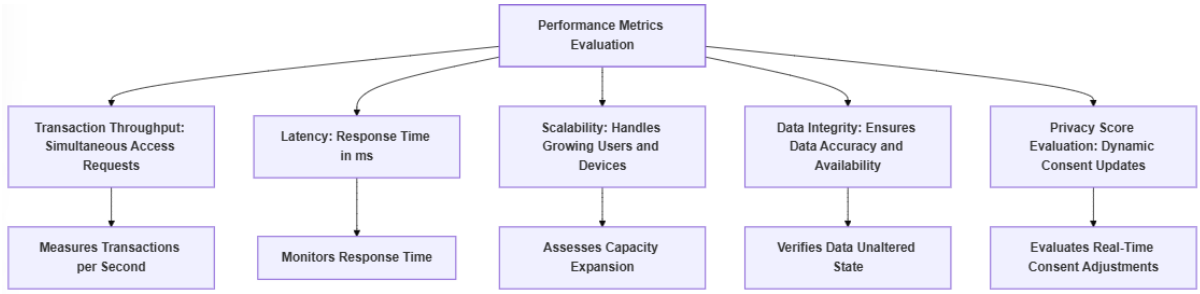


Figure 4. 22: Performance Metrics Evaluation Diagram Summarising Throughput, Latency, Scalability, and Integrity Metrics

4.3.3 Implementation and Validation Framework Design

The implementation and validation framework builds upon the technical infrastructure outlined in Table 3.1, integrating advanced components to ensure robust privacy preservation and secure data handling in smart home healthcare environments. Central to the design is an enhanced security layer that incorporates PyCryptodomex for hybrid ECC-256r1 and AES-128 encryption, ensuring end-to-end data confidentiality. Data aggregation and encryption are managed through a home gateway configured for high-speed secure transmission, while Pinata gateway integration with IPFS provides off-chain storage with redundant data availability, efficient retrieval, and secure content addressing.

Validation of the system operates across four interdependent domains to guarantee its reliability and security. Functional validation involves verifying core components such as role-based access control, privacy score calculations, and dynamic consent management using the Hardhat Testing Suite. Security validation ensures cryptographic implementation and smart contract functionality through rigorous vulnerability assessments, access control verification, and gas optimisation checks. Integration testing evaluates component interactions across IoT devices, blockchain networks, and the system’s frontend-backend architecture, focusing on data flow consistency and smart contract event handling. Emergency protocols are also tested for rapid authentication, priority request handling, and multi-user access management, ensuring the framework's resilience under high-demand scenarios.

This design approach provides a comprehensive foundation for system verification, ensuring that privacy, security, and interoperability are maintained throughout the framework. The validation architecture lays the groundwork for further testing and evaluation, detailed in

Chapter 6, where the system's effectiveness and compliance with healthcare standards will be rigorously assessed.

4.4 User Privacy Features and Controls

The privacy features and control mechanisms designed within the framework establish a user-centric, privacy-preserving architecture. By leveraging dynamic privacy scoring to assess privacy sensitivity, the MDDC model facilitates context-aware, adaptive consent management. These mechanisms are integrated into blockchain-based smart contracts to ensure transparent, enforceable access control. This system ultimately empowers users to maintain control over their health data while enabling secure and ethical data sharing.

4.4.1 Privacy Control Architecture

The privacy control architecture is grounded in three critical components: dynamic privacy scoring, user-centric controls, and consent flow management. The privacy scoring mechanism, detailed in Section 4.2.1, combines time-decay factors, role-based weights, and data sensitivity metrics to enforce adaptable privacy levels. Table 4.5 summarises the sensitivity levels and their application contexts. This dynamic mechanism enables granular permission management, real-time score adjustments, and automated threshold monitoring, ensuring a robust framework for data protection.

Table 4. 5: Privacy Score Component Weights and Sensitivity Levels

Component	Weight Range	Application Context
Time Decay (λ)	0.1 - 1.0	Recent to Historical Data
Role-Based (ωr)	0.5 - 0.9	User Role Hierarchy
Data Sensitivity (γd)	0.3 - 0.9	Data Type Classification

Figures 4.23 and 4.24 illustrate the hierarchical relationship between privacy components and role-based access control mechanisms, respectively. By employing smart contract enforcement, context-aware adjustments, and real-time consent updates, the MDDC principles underpin dynamic privacy scoring and comprehensive consent management. The React-based user interface offers an intuitive dashboard for managing data sharing, adjusting privacy policies, and responding to access requests. This frontend integration ensures transparency and usability, keeping users informed of data interactions.

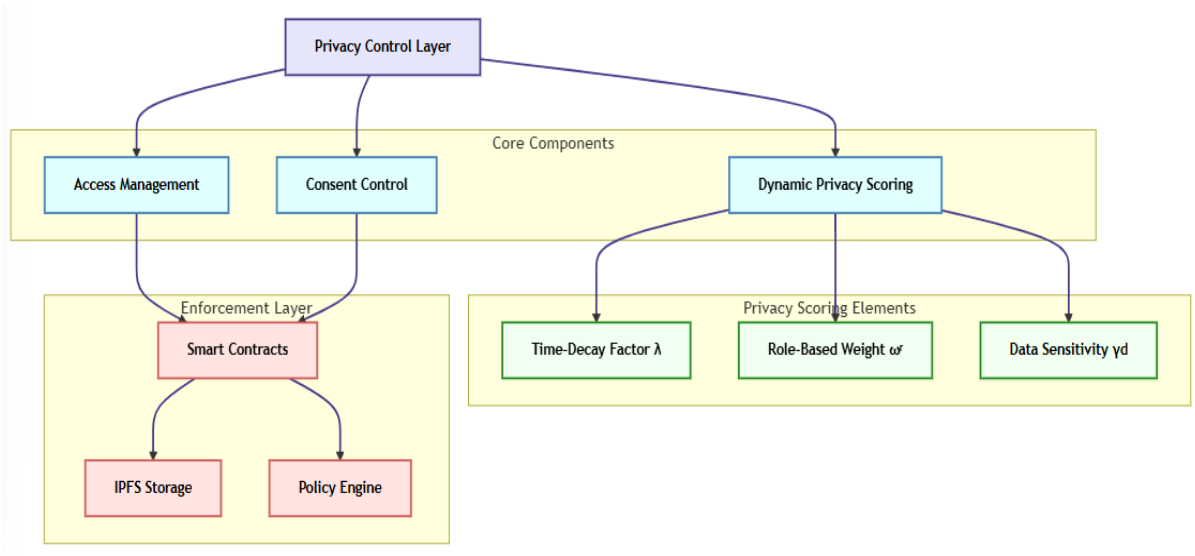


Figure 4. 23: Privacy Control Architecture Components

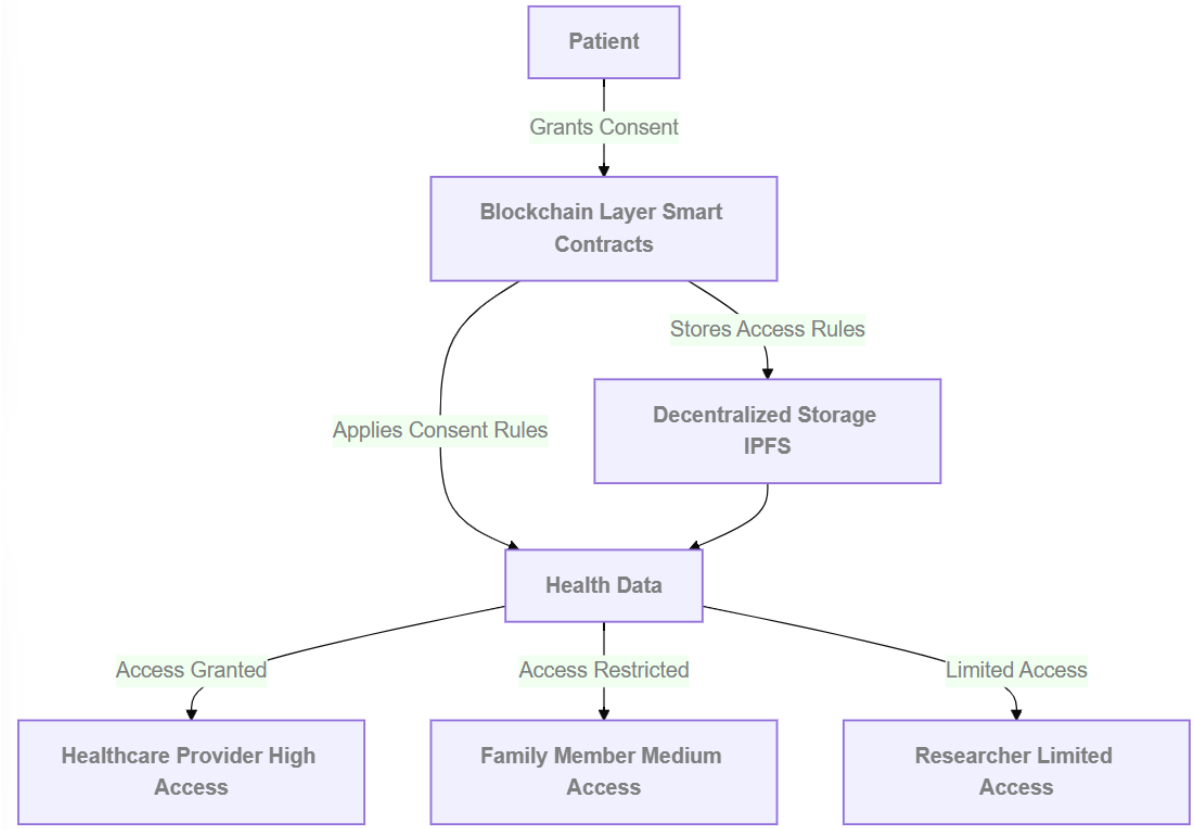


Figure 4. 24: Data Sensitivity and Role-Based Access Control Mechanism

4.4.2 Transparency and Audit Mechanisms

To address gaps in healthcare data transparency, the framework incorporates blockchain-based audit trails. These immutable logs record data access events, privacy modifications, and consent activities, ensuring verifiability and user accountability. Figure 4.25 illustrates the audit trail architecture, where all interactions are recorded on the blockchain and accessible via both patient and provider dashboards. Events such as HealthDataSent and PatientConsentToRI are logged, creating tamper-proof records of interactions.

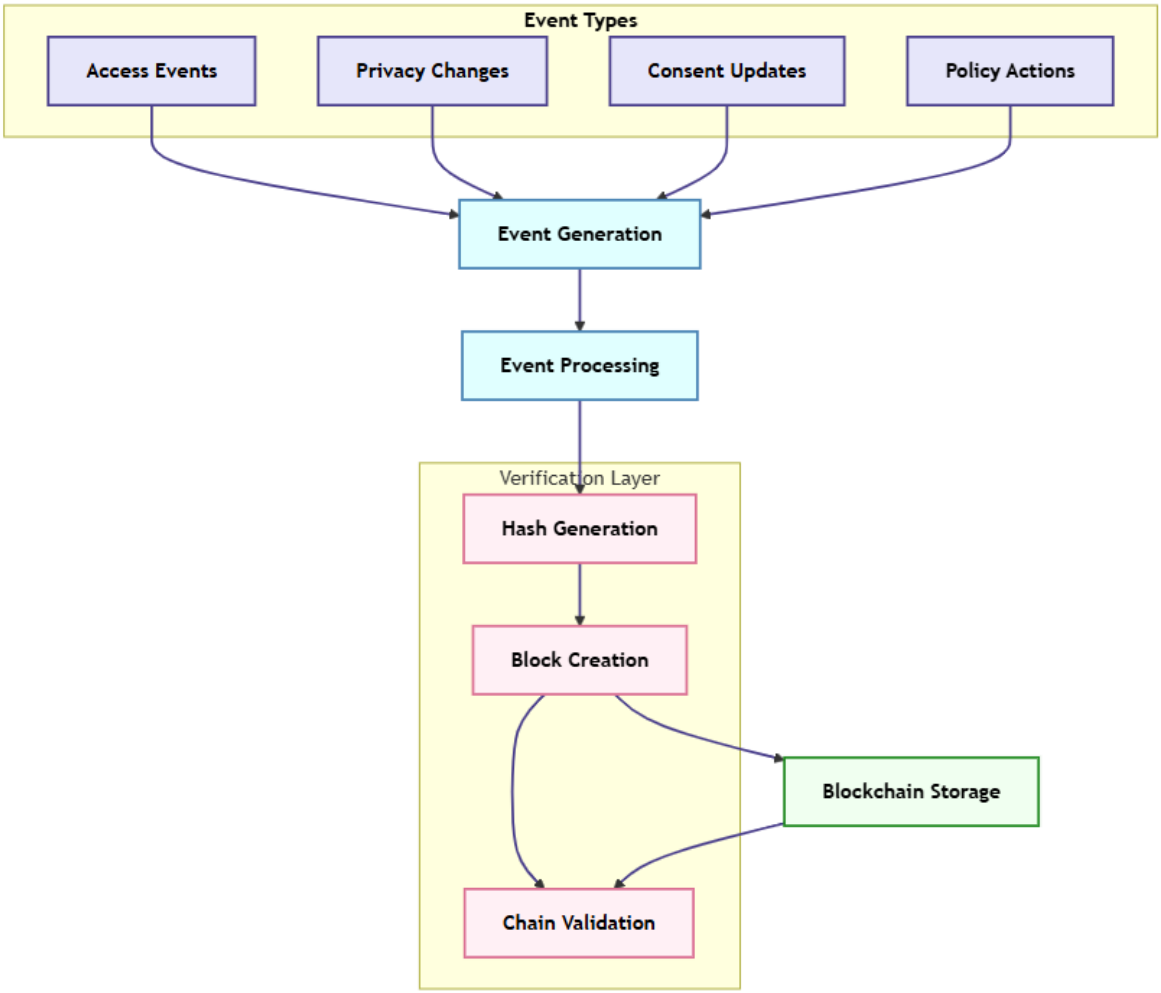


Figure 4. 25: Audit Trail Architecture

Real-time notification systems further enhance transparency, providing users with alerts for access attempts, privacy score changes, and consent modifications. Figure 4.26 depicts the system's notification interface, highlighting priority-based alerts and user preferences. The system's user interface demonstrates a thoughtful implementation of privacy-aware healthcare data management through three key interactive screens. The dashboard provides users with a

comprehensive overview of data access activities and privacy metrics, enabling real-time monitoring of data utilization. The data-sharing controls facilitate granular permission management, allowing users to define and modify access parameters for different healthcare stakeholders. The access request management interface streamlines the consent process by presenting incoming requests with contextual information, supporting informed decision-making while maintaining compliance with privacy regulations. This interface design emphasises both usability and security, ensuring that complex privacy controls remain accessible to users of varying technical expertise.

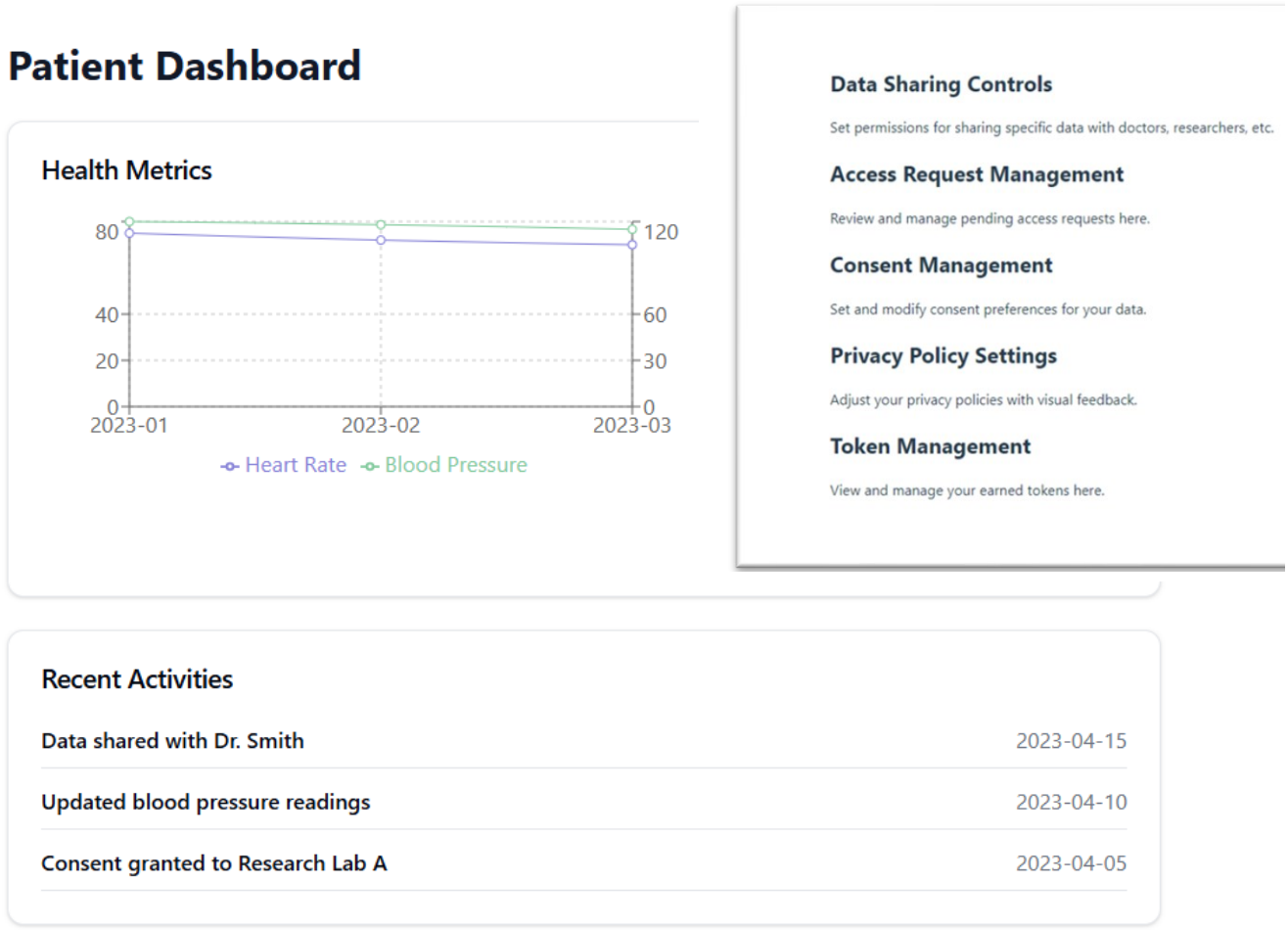


Figure 4. 26: User Interface Key Screens from the React Frontend, such as the Dashboard, Data Sharing Controls, and Access Request Management.

The audit mechanism, as shown in Figure 4.27, combines cryptographic event logging with user-friendly dashboards, enabling data owners to monitor and control access effectively. This comprehensive design empowers users by reinforcing data ownership, privacy, and security. Through a blend of dynamic privacy scoring, encryption, consent management, and

blockchain-driven transparency, the framework delivers a cutting-edge solution for ethical data sharing in healthcare.

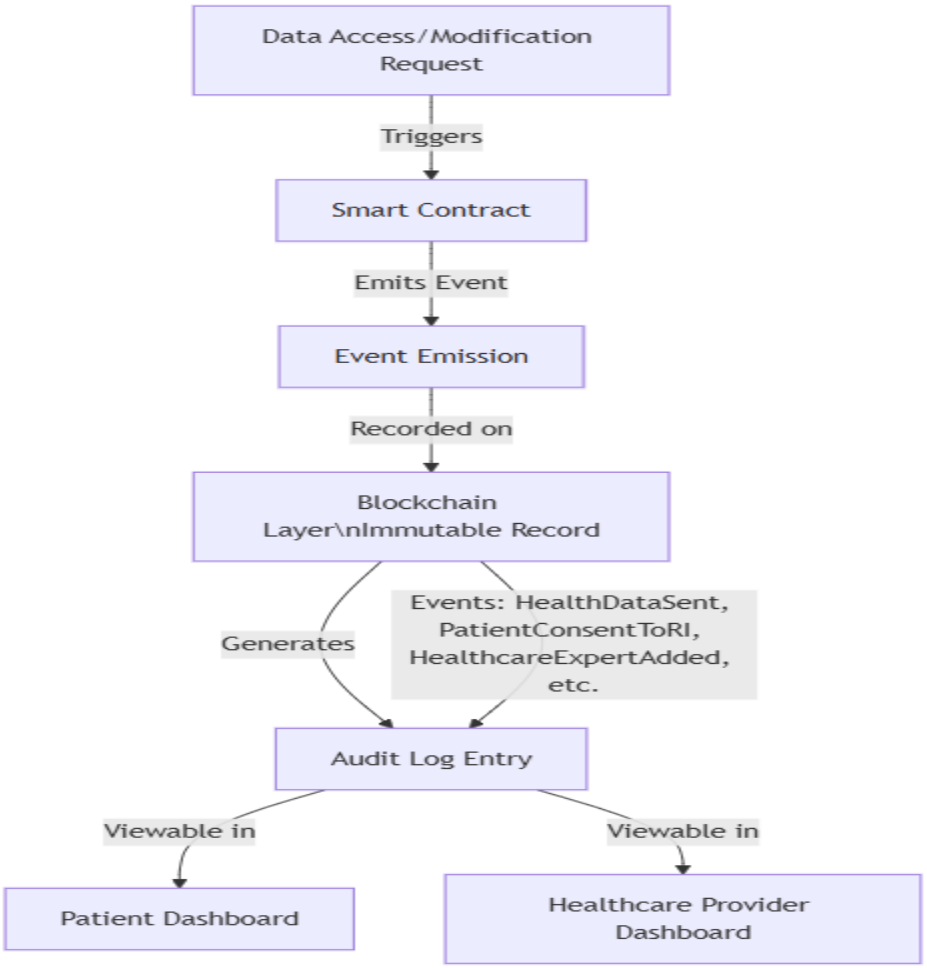


Figure 4. 27: Audit Trail and Transparency in Data Access Control

4.4.3 Privacy Score and Dynamic Consent Management

The framework's design integrates dynamic privacy scoring with a user-centric consent management system, enabling real-time adaptability to changing healthcare scenarios. Unlike static metrics, the privacy score evolves dynamically by incorporating multiple contextual factors, including data sensitivity, role-based weights, and time-specific adjustments. This dynamic approach reflects the complexities of healthcare data sharing, ensuring access permissions align with user-defined privacy preferences while adapting to real-time needs. For instance, as privacy scores fluctuate, the system initiates protective measures for low scores and temporarily elevates permissions during emergencies, maintaining accountability through

comprehensive audit trails. Figure 4.28 illustrates the dynamic privacy score calculation and consent adjustment workflow.

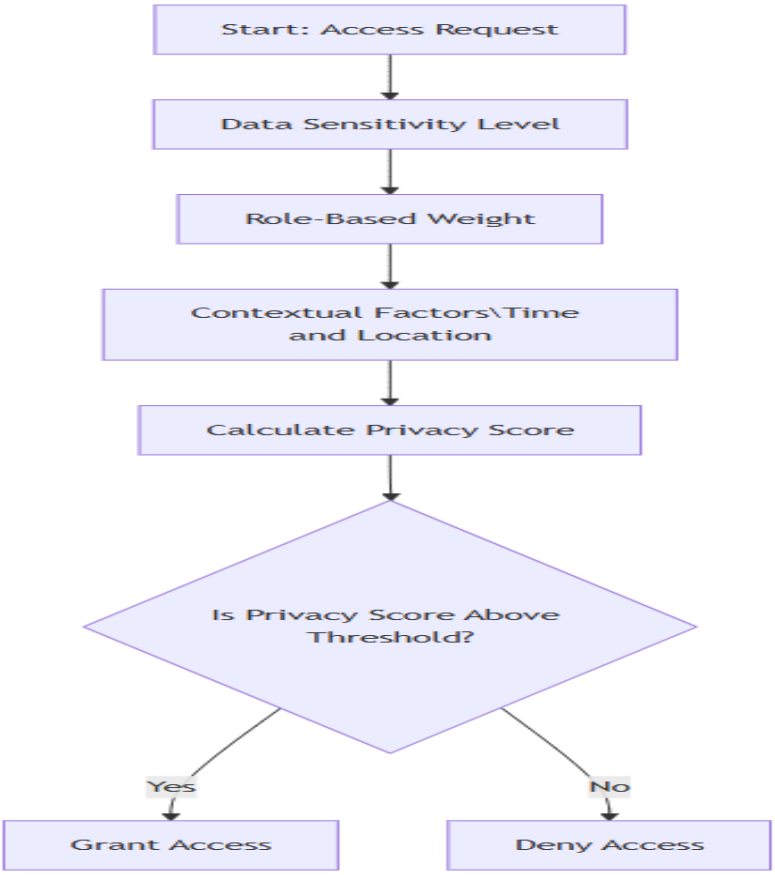


Figure 4. 28: Dynamic Privacy Score Calculation and Consent Adjustment.

The consent management system embodies granular, scenario-specific authorisations, empowering users to tailor access permissions to their immediate healthcare needs. From routine consultations to emergency scenarios, the system ensures precise and context-aware adjustments. Figure 4.29 depicts the decision-making process from access request to final authorisation, integrating both user-defined preferences and automated mechanisms. This adaptive architecture enables seamless healthcare delivery while prioritising privacy protections.

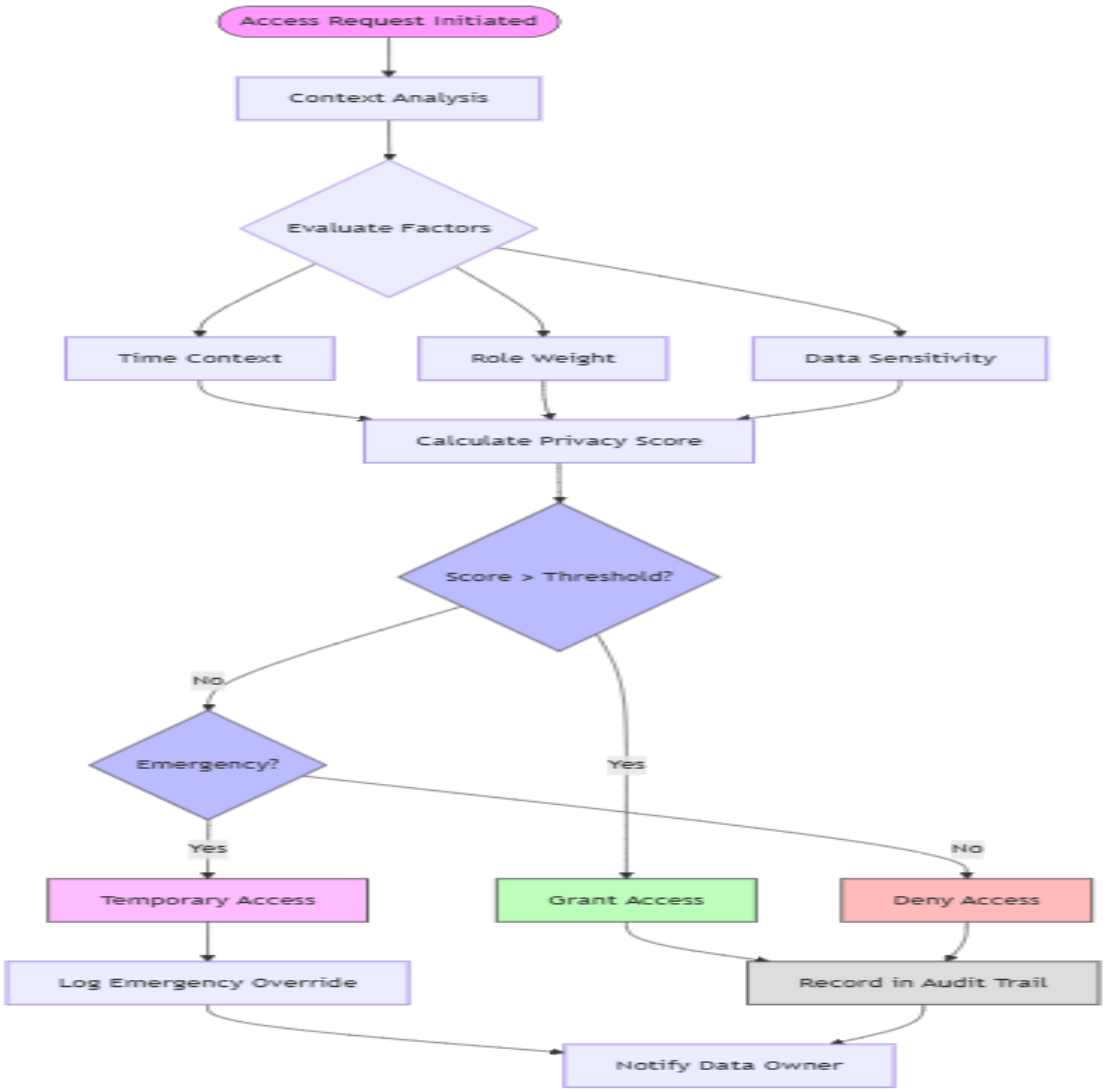


Figure 4. 29: Consent Management Workflow

The framework's architecture balances stringent privacy controls with healthcare accessibility. Real-time adjustments to privacy scores, supported by robust processing capabilities, ensure consistent system performance. The effectiveness of this approach is demonstrated by its capacity to maintain accuracy, stability, and scalability while managing dynamic consent modifications. Figure 4.30 highlights the core architectural components designed to optimise performance and adaptability, establishing a strong foundation for addressing modern healthcare privacy challenges.

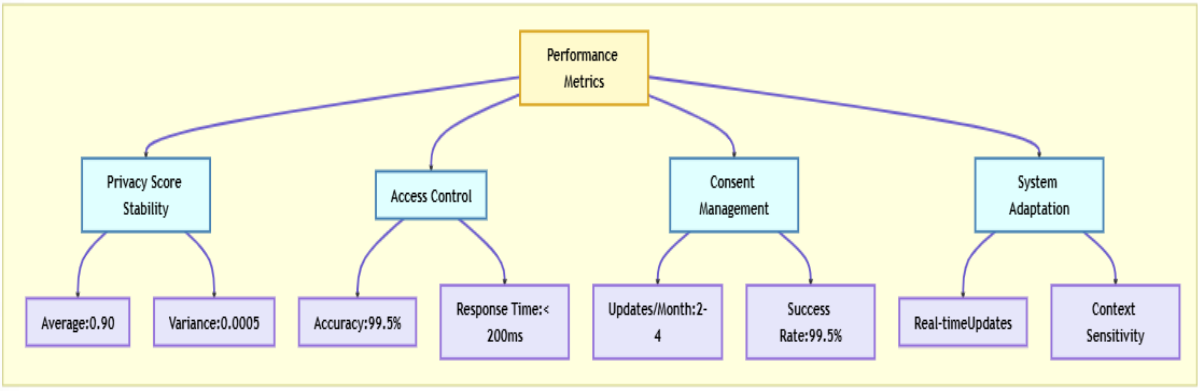


Figure 4. 30: Privacy Score Performance Metrics.

4.4.4 Security Integration Framework

The security architecture seamlessly integrates privacy controls with advanced encryption mechanisms, ensuring secure data sharing without compromising performance. A hybrid encryption scheme, combining ECC-256 and AES-128, forms the foundation for secure and efficient data exchange in healthcare environments. This integration is visually detailed in Figure 4.31, which depicts the security-privacy integration architecture.

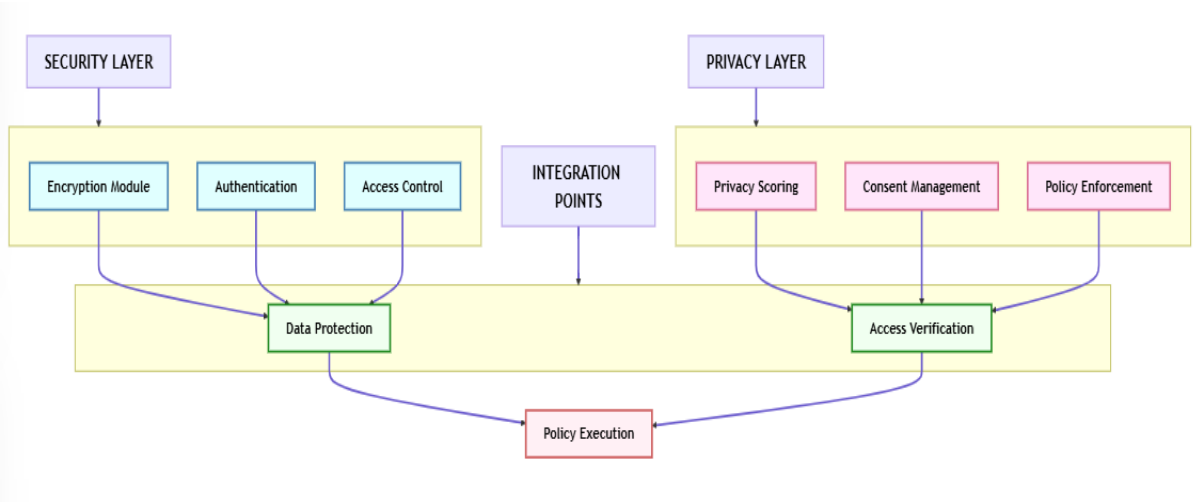


Figure 4. 31: Security-Privacy Integration Architecture.

Key innovations include the integration of dynamic privacy scoring with blockchain-enforced access control, allowing real-time evaluation of access policies through smart contract templates. Contextual adjustments to privacy settings enable healthcare scenario-specific adaptations, environmental evaluations, and temporal modifications, ensuring data access remains precise and secure. The audit system leverages the blockchain's immutability to create

tamper-proof logs, supporting real-time monitoring and privacy-preserving logging mechanisms. Flexible privacy policies allow dynamic enforcement of user preferences and context-aware rule modifications, enabling a modular and adaptive framework.

The hybrid encryption architecture, shown in Figure 4.32, underscores the modularity of the proposed design, allowing future enhancements while preserving privacy. This design harmonises security requirements with usability considerations, providing a scalable and robust framework for real-world healthcare scenarios. By combining advanced encryption, dynamic privacy scoring, and blockchain-driven transparency, the framework establishes a secure and user-centric approach to healthcare data management.

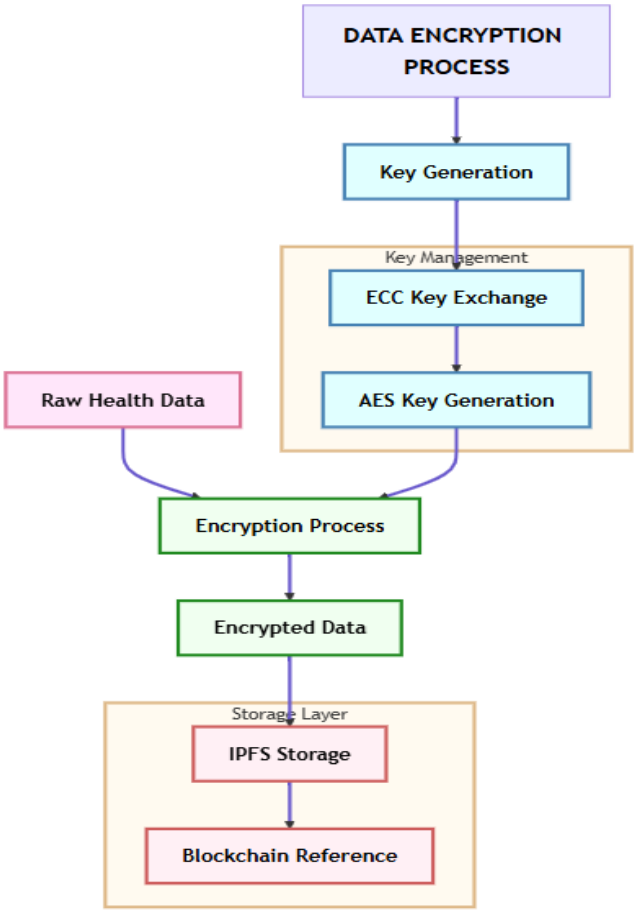


Figure 4. 32: Hybrid Encryption Architecture

4.5 Security and Privacy Safeguards

The security and privacy safeguards embedded in this framework employ a multi-layered approach to protect sensitive healthcare data. The system's design integrates robust encryption,

role-based access control, audit mechanisms, and compliance with regulatory standards, ensuring confidentiality, integrity, and availability.

4.5.1 Data Encryption and Confidentiality

The framework utilises a hybrid encryption model combining ECC-256 for secure key exchange and AES-128 in EAX mode for data encryption, ensuring efficient and secure data handling (Popoola O. , et al., 2024). Data transmitted between IoT devices, the backend, and storage layers is securely exchanged using ECC-256 for key exchange and encryption during transit, with SHA-512 for message integrity verification, while AES-128 in EAX mode ensures the confidentiality and integrity of data stored at rest in IPFS storage. This lightweight yet highly secure encryption model balances computational efficiency with stringent security requirements, as detailed in Figure 4.33. The hybrid workflow ensures robust protection against cyber threats while maintaining compatibility with energy-efficient healthcare IoT devices.

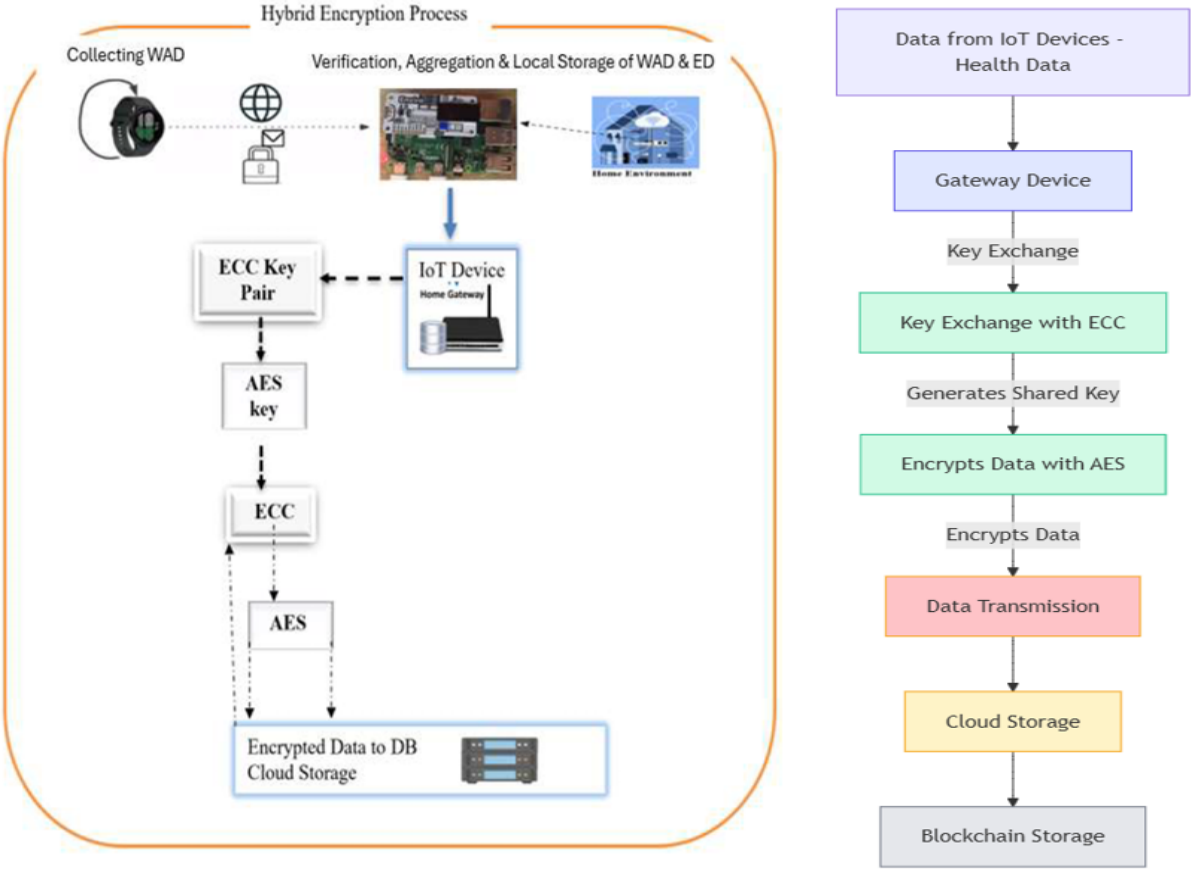


Figure 4. 33: Encryption Workflow Using Hybrid ECC-256/AES-128

4.5.2 Access Control and Data Integrity Mechanisms

Role-Based Access Control (RBAC) enforces the least privilege principle through smart contract-based templates that dynamically adjust permissions based on privacy scores. Blockchain technology ensures data integrity by providing an immutable audit trail of all system interactions, preventing unauthorised modifications. The logging and auditing system further supports traceability by recording events such as data access and consent changes, as depicted in Figure 4.34. The events in the MDDC Consent Manager Contract track critical system activities such as data access and privacy updates. These events provide transparency and facilitate audit trails for smart contract interactions.

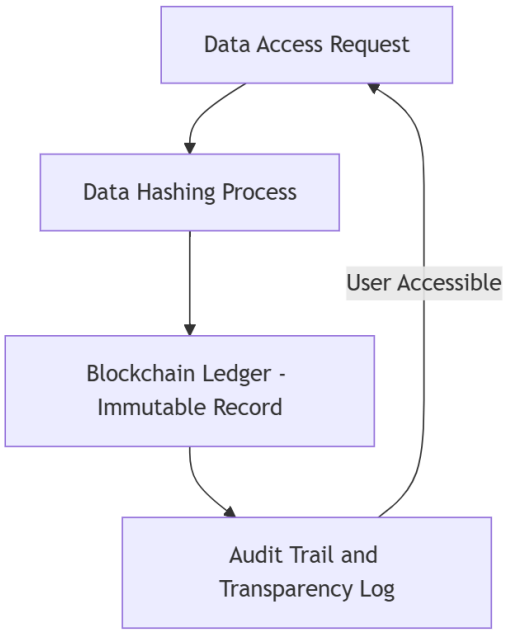


Figure 4. 34: Data Integrity Workflow and Audit Trail

4.5.3 Regulatory Compliance Architecture

The system adheres to GDPR, HIPAA, and other international data protection standards through a multi-layered compliance framework. Measures include data minimisation, purpose limitation, and support for user rights such as data access, modification, and portability. The decentralised IPFS storage system underpins these rights, ensuring data availability and compatibility with regulatory requirements. Table 4.6 summarises the compliance measures, while Figure 4.35 outlines the system's compliance architecture.

Table 4. 6: Compliance Measures Summary

Regulatory Requirement	Compliance Measure	Design Specifications
Data Minimisation	Limited Data Collection	Only essential data is collected and used.
Purpose Limitation	Purpose-Specific Consent	Data is used only for approved healthcare purposes.
User Rights	Access, Modify, Delete Options	Users can access, modify, or delete their data at any time.
Data Portability	IPFS-Based Data Retrieval	Data is stored in a portable format for user access.
Transparency	Audit Logs and Documentation	Provides audit logs and policy documentation for transparency.

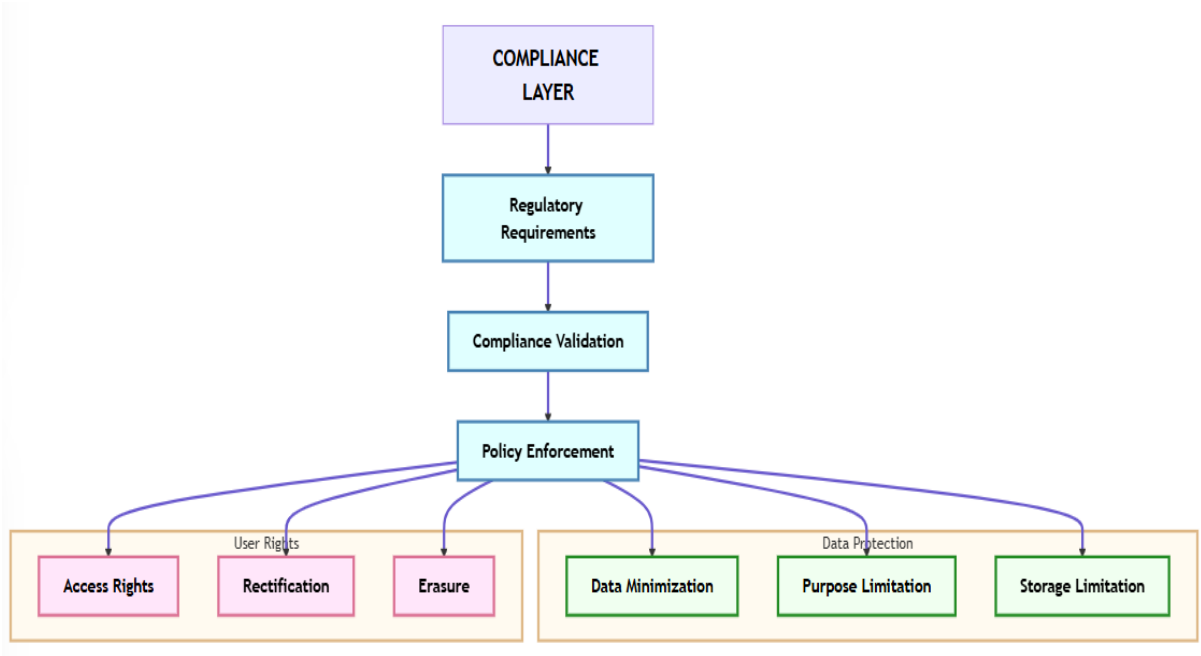


Figure 4. 35: Regulatory Compliance Framework

4.5.4 Privacy Score Effectiveness

The privacy score mechanism ensures that access decisions dynamically adapt to user preferences and healthcare contexts. Continuous validation monitors privacy score stability, access control accuracy, and consent management effectiveness. Figure 4.36 illustrates the flow of data through the privacy score calculation process, integrating role-based weights, data sensitivity levels, and contextual adjustments. Automated consent updates and real-time monitoring enhance the system's adaptability to dynamic scenarios, ensuring privacy protections align with user-defined thresholds.

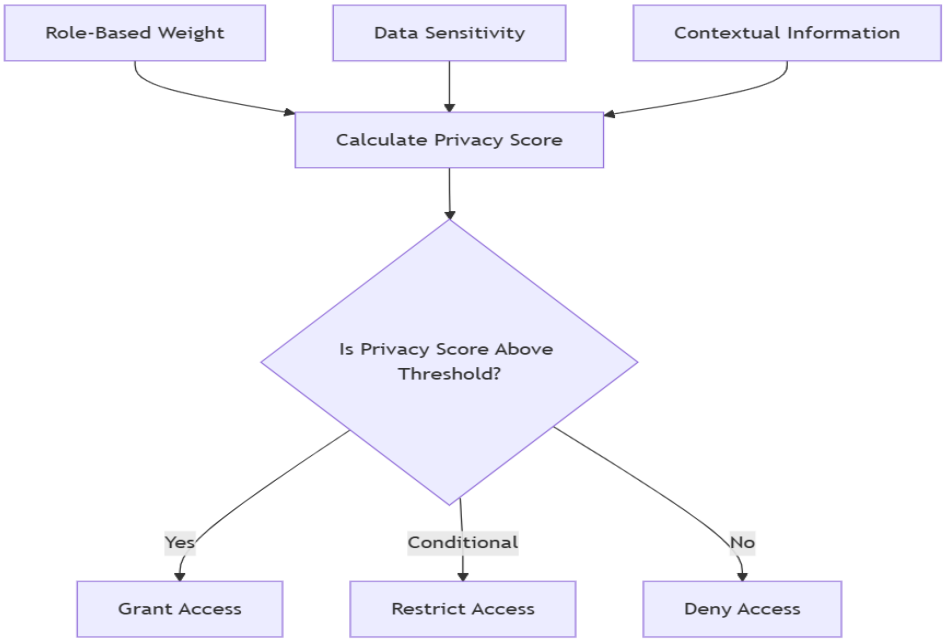


Figure 4. 36: Privacy Score Calculation and Adaptation

4.6 Conclusion

This chapter outlined the design and architecture of the Privacy-Aware Authorisation Framework, a novel approach aimed at addressing the challenges of healthcare data privacy in smart home environments. By integrating robust data security mechanisms with user autonomy, the framework advances ethical data disclosure, ensuring a balance between privacy protection and user control.

4.6.1 Summary of Architectural Decisions

The framework's architectural design integrates hybrid encryption (ECC-256 for key exchange and AES-128 for data encryption) to ensure data confidentiality and integrity while maintaining computational efficiency, particularly for resource-constrained IoT devices. Blockchain-based access logging enhances transparency and immutability, allowing users to monitor data access securely. Additionally, role-based access control enforced through smart contracts dynamically adapts permissions based on privacy scores, upholding the principle of least privilege. These decisions collectively create a secure and adaptive environment for managing healthcare data privacy.

4.6.2 Alignment with Privacy Principles

Grounded in key privacy principles i.e., user autonomy, data minimisation, purpose limitation, and transparency, the framework empowers users to manage data sharing through dynamic privacy controls. The blockchain-based audit trail provides a tamper-proof log of access requests, ensuring transparency and user empowerment in alignment with GDPR requirements. Data minimisation is achieved through selective information sharing based on predefined privacy scores, ensuring only essential data is disclosed under controlled conditions.

4.6.3 Framework Effectiveness

The architectural framework effectively embeds privacy controls within the core system while maintaining performance and usability. This demonstrates that robust privacy protection can coexist with efficient healthcare service delivery. The incorporation of dynamic privacy controls for regulating access based on contextual sensitivity and smart contracts enforced privacy-preserving policies securely deployed on a blockchain network to ensure transparent and immutable healthcare data management illustrated in Figure 4.37 represents a foundational step toward reimagining healthcare data management. This chapter lays the groundwork for implementation strategies (Chapter 5) and system evaluation (Chapter 6), ensuring that privacy protection is both practical and sustainable in the era of smart home healthcare.

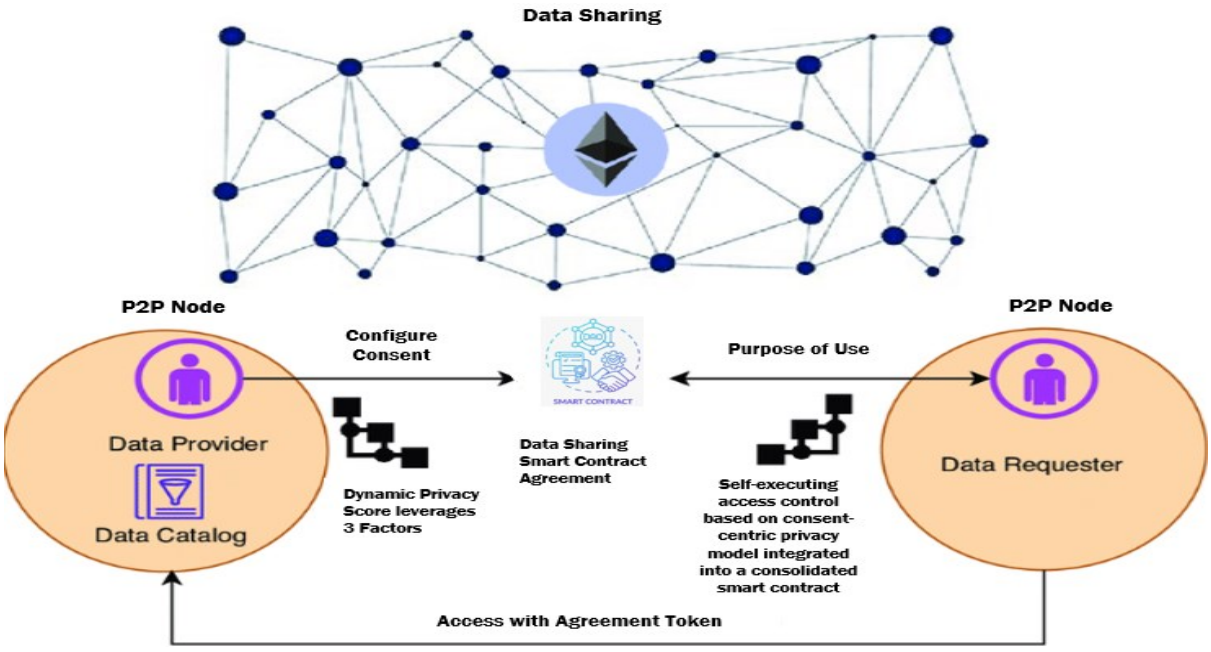


Figure 4. 37: Overview of the Proposed Implementation and Integration of Blockchain Technology, Smart Contracts, And Dynamic Privacy Controls.

Chapter 5

5. Implementation and System Integration

This chapter details the practical implementation and system integration of the privacy-aware authorisation framework developed in Chapter 4. The framework is designed to enable secure, patient-centric healthcare data management by integrating key components such as the Dynamic Privacy Scoring Model, Multi-Dimensional Dynamic Consent Model (MDDC), smart contract-based access control, and decentralised storage solutions.

The implementation is grounded in blockchain technology, specifically leveraging the Ethereum blockchain and the InterPlanetary File System (IPFS) for decentralised storage. Smart contracts automate privacy scoring and consent management, ensuring secure, transparent, and efficient management of encrypted health data. The system's architecture enables patients to exercise granular control over their health data, maintaining both privacy and system security.

The system is structured around a single local Hardhat Ethereum Network (HEN) with multiple addresses, where addresses are assigned to network participants such as the Smart Home, Storage, Healthcare Institution, Family Member, and Research Institute. These network entities represent nodes and collectively ensure the transparent and secure data flow among patients, caregivers, healthcare providers, and research institutes. User interactions are managed via a web interface that provides real-time updates on consent preferences and access history.

To validate the applicability, responsiveness, and resilience of the developed privacy-aware authorisation framework, a structured role-play exercise was conducted involving key stakeholders i.e., patients, healthcare providers, researchers, and family members. Each stakeholder enacted realistic interaction scenarios representative of typical system usage patterns, enabling comprehensive testing of the framework’s dynamic access control, privacy scoring mechanisms, and user-centric interfaces. This simulation approach facilitated the identification and refinement of critical operational attributes, ensuring the implemented framework accurately addresses stakeholder requirements and demonstrates robust, responsive behaviour under varied real-world conditions.

Figure 5.1 illustrates the high-level architecture of the privacy-aware framework. The Ethereum blockchain serves as the core layer for transaction logging and policy enforcement, while IPFS facilitates off-chain storage of encrypted data. A React-based frontend, supported by Web3.js, enables end-users to interact seamlessly with the system, ensuring real-time consent and privacy management.

This architectural foundation builds upon the theoretical framework detailed in Chapter 4, providing a practical implementation that balances privacy preservation with usability and scalability. The implementation encountered several challenges, including computational overhead, scalability constraints, and security vulnerabilities, which are discussed in detail in Section 5.3.4.

5.1 Development Environment and Tools

This section presents the development framework and tools employed in realising the privacy-aware system. Building on the architectural principles discussed in Chapters 3 and 4, it outlines the practical integration of key components and methodologies that underpin the system's functionality.

The architecture integrates the Ethereum blockchain for access control, IPFS for decentralised data storage, and a React-based interface to enable user interaction. IoT devices collect data, which is encrypted and securely transmitted via gateways to the blockchain for processing. Smart contracts enforce privacy preferences and consent mechanisms, while IPFS ensures scalable and secure storage of sensitive data. This design supports decentralised, transparent, and user-centric management of healthcare data.

Stakeholder engagement plays a pivotal role in the system. Patients, healthcare providers, and researchers interact with the framework based on predefined roles encoded in smart contracts. Each interaction generates unique transaction hashes, recorded on the blockchain to create a transparent audit trail that ensures data integrity and immutability. This process, depicted in Figure 5.2, highlights the system's ability to facilitate secure and accountable data sharing.

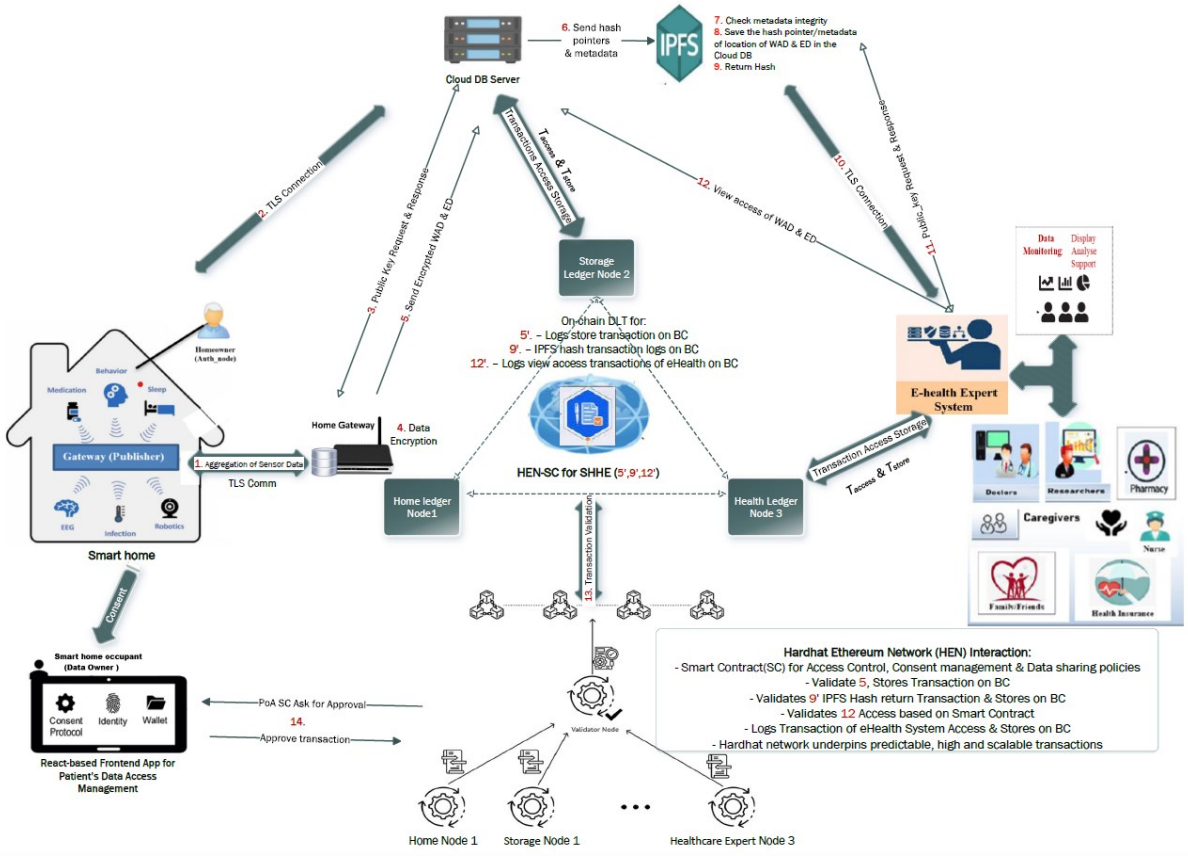


Figure 5. 1: Overview of Privacy-Aware Framework

Legend for Figure 5.1: Overview of Privacy-Aware Framework

1. **TLS Connection Establishment** – Secure session setup between smart home and cloud database.
2. **Public Key Request & Response** – Data encryption key exchange for secure transmission.
3. **Secure Encrypted Message Exchange** – Transmission of encrypted health data.
4. **Data Encryption** – Patient data is encrypted before integration into the blockchain.
5. **Log Storage Transaction on Blockchain** – Ensuring immutability of access logs.
6. **Send Hash Pointers & Metadata** – Metadata integrity check on IPFS.
7. **Check Metadata Integrity** – Ensuring correctness before storing pointers.
8. **Save Hash Pointers in Cloud DB** – Reference to encrypted data stored off-chain.
9. **Return Hash to Requestor** – Providing a reference to securely stored data.
10. **Transaction Storage on Blockchain** – Logging all access transactions.
11. **Secure TLS Connection to Expert System** – Establishing a private communication channel.
12. **Log View Access Transactions** – Storing audit logs on blockchain.
13. **Transaction Access Storage** – Updating access logs in the system.
14. **Approval Transaction on React-based Frontend** – Patient consents to data access requests.

The tools employed in the system's development as detailed in Table 3.1 in Chapter 3, provide a robust foundation for its implementation. The React framework supports the creation of an intuitive frontend interface, and IPFS enhances data storage efficiency and scalability. Although these tools and methodologies were introduced in Chapter 4, their integration in this implementation underscores the system's scalability, compatibility, and user-centric approach. The overarching framework ensures secure data handling and transparent engagement, paving

the way for the detailed implementation of privacy scoring and consent management in subsequent sections.

Figure 5.2 illustrates the stakeholder engagement model, where transaction hashes provide a verifiable audit trail for all activities. This mechanism ensures accountability and upholds the integrity of data interactions across the system.

The development environment and architecture collectively provide a comprehensive foundation for implementing the privacy-aware framework. By leveraging decentralised storage, blockchain-based automation, and user-friendly interfaces, the system achieves a seamless balance between privacy, security, and usability.

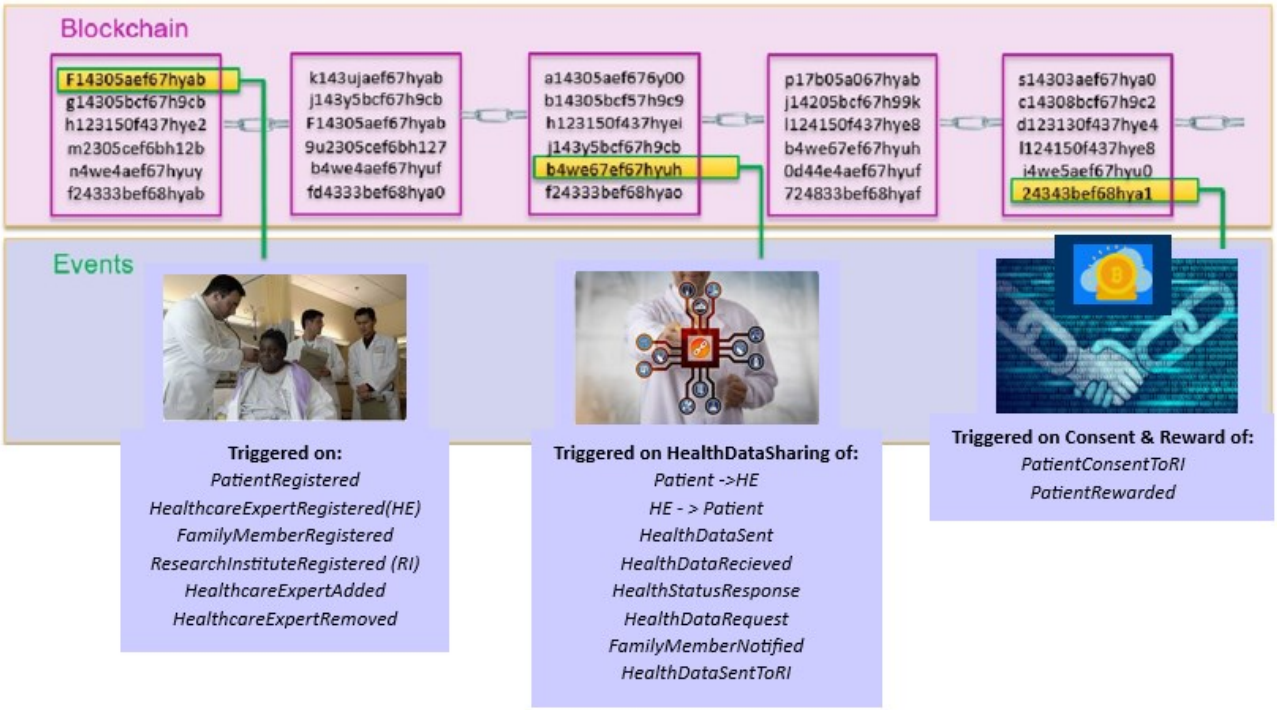


Figure 5. 2: Stakeholders' Engagement Model

5.2 Implementation of the Dynamic Privacy Scoring Model

The implementation of the Dynamic Privacy Scoring Model operationalises the theoretical framework described in Chapter 4. By embedding the model into the privacy-aware system architecture, the implementation ensures real-time computation, automated enforcement of privacy preferences, and seamless interoperability with other system components. This section elaborates on how the model was developed, integrated, and optimised within the broader framework.

5.2.1 Overview of the Model

The Dynamic Privacy Scoring Model was implemented as part of the Ethereum blockchain smart contract. Using Solidity, the smart contract encodes the privacy scoring formula, incorporating key factors such as the Time-Decay Factor (λ), Role-Based Weight Factor (ω_r), and Data Sensitivity Factor (γ_d). This formula dynamically adjusts privacy scores based on real-time contextual data, enabling adaptive enforcement of privacy preferences. The implementation was designed to evaluate access requests immediately, leveraging blockchain automation to eliminate manual intervention. Every access decision, including denials, is recorded immutably on the blockchain, ensuring complete auditability and compliance.

The smart contract logic was optimised to minimise computational overhead, thereby reducing transaction gas costs. Key functions, such as `evaluateAccessRequest` and `computePrivacyScore`, were streamlined to ensure efficiency while maintaining robustness. This implementation not only enforces privacy preferences but also provides transparency through the blockchain's immutable records. A detailed explanation of the smart contract and its deployment can be accessed through the GitHub repository. Figure 5.3 illustrates the logical flow within the smart contract, depicting the sequential steps of access request validation, privacy score computation, consent verification, and access decision execution.

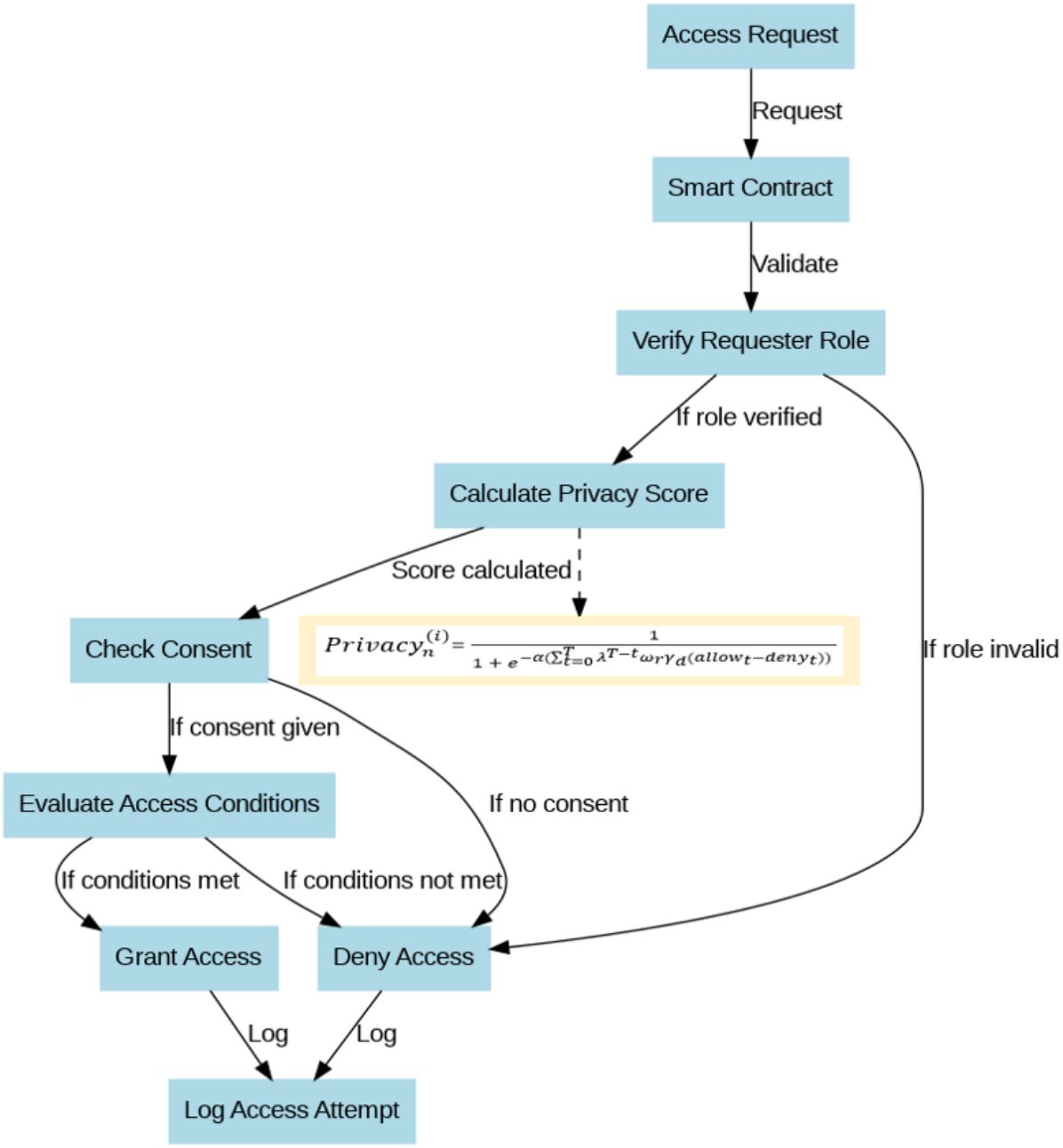


Figure 5. 3: Smart Contract Logic for Dynamic Privacy Scoring

5.2.2 Integration with System Architecture

The Dynamic Privacy Scoring Model is seamlessly integrated into the system's multi-layered architecture, connecting various components to enable dynamic privacy management. IoT devices collect and transmit contextual metadata, which is utilised by the privacy scoring system to evaluate access permissions in real time. The computed privacy scores are then applied to enforce access control decisions for data stored in the decentralised IPFS

infrastructure. By embedding the scoring model into the smart contract, the system ensures that these decisions are both transparent and secure.

The React-based frontend interface allows users to adjust data sensitivity settings, which directly influence privacy scores and subsequent access outcomes. This integration empowers end-users with granular control over their data-sharing preferences. Moreover, the modular design of the system architecture ensures that the scoring model remains interoperable with other components, including decentralised storage, blockchain nodes, and stakeholder interfaces, enabling a cohesive and adaptable framework for privacy management.

5.2.3 Mapping Privacy Scores to Access Control

The Dynamic Privacy Scoring Model operationalises access control policies by aligning privacy scores with predefined thresholds for stakeholder roles and data types. Each privacy score dynamically adjusts based on the sensitivity of the data being requested, the role of the stakeholder, and the contextual factors associated with the request. For instance, highly sensitive medical records are accessible only to healthcare providers with a critical role, while researchers are limited to anonymised data unless explicit consent is provided. This adaptive approach ensures that access decisions reflect ethical and contextual considerations, thereby balancing privacy with utility.

Table 5.1 provides a detailed mapping of privacy scores to stakeholder roles and data types, demonstrating how these scores govern access levels. It highlights the system's ability to enforce privacy preferences dynamically, ensuring that only authorised entities can access specific categories of data. This mapping operationalises the theoretical principles discussed in Chapter 4, embedding them into the functional system to address real-world data-sharing scenarios.

Table 5. 1: Mapping of Stakeholder Roles to Privacy Scores

Data Type	DSF(γd)	RBWF (ω_r)	Privacy Score Range	Access Level
Medical History	0.9	Doctor: 0.9	0.729 – 0.81	Full Access (if consented)
		Family Member: 0.7	0.567 – 0.63	Limited Access
		Researcher: 0.5	0.405 – 0.45	Anonymised Data Only
Medication	0.7	Doctor: 0.7	0.441 – 0.49	Partial Access
		Family Member: 0.5	0.315 – 0.35	Limited Access
		Researcher: 0.3	0.189 – 0.21	Anonymised Data Only
Lifestyle Data	0.5	Doctor: 0.6	0.27 – 0.30	Partial Access
		Family Member: 0.5	0.225 – 0.25	Limited Access
		Researcher: 0.2	0.09 – 0.10	Anonymised Data Only
Environmental Data	0.3	Doctor: 0.5	0.135 – 0.15	Limited Access
		Family Member: 0.4	0.108 – 0.12	Limited Access
		Researcher: 0.2	0.054 – 0.06	Anonymised Data Only

5.2.4 Challenges and Mitigation

The implementation of the Dynamic Privacy Scoring Model encountered several challenges, including computational overhead, scalability constraints, and security vulnerabilities. Real-time computation of privacy scores introduced latency, particularly during high transaction volumes, which was mitigated through optimizing the deployed smart contract and Cloud based decentralised storage (IPFS) to act in similitude to Layer-2 scaling solutions. These solutions offloaded computationally intensive processes, significantly reducing gas costs and improving response times. Additionally, the smart contract logic was optimised to eliminate redundant operations, enhancing the system's overall efficiency.

Scalability was further addressed by decentralising storage using IPFS, which alleviated the on-chain storage burden while ensuring data integrity. End-to-end encryption was implemented to secure communication between IoT devices and the blockchain, protecting sensitive metadata and mitigating security vulnerabilities. By employing caching mechanisms for frequently accessed data, the system achieved a balance between performance and privacy, ensuring that privacy scores could be computed and enforced dynamically without compromising scalability or security.

5.3 Implementation and System Integration of Consent Management

The MDDC translates theoretical constructs into an operational framework for real-time consent management. This implementation is achieved through the integration of smart contracts, frontend interfaces, and decentralised storage, enabling dynamic consent evaluation and enforcement.

5.3.1 Smart Contract Implementation for Consent Management

The implementation of the *HealthDataSharing* smart contract plays a pivotal role in enabling dynamic consent evaluation and role-based access control within the privacy-aware framework. This section outlines the deployment process, contract functionalities, and key integration aspects, ensuring a comprehensive understanding of its operational significance.

The smart contract development and deployment leveraged the Hardhat Ethereum Network (HEN), which provided a robust environment for simulating blockchain operations. The development process involved setting up a structured project environment in Hardhat, writing the contract in Solidity, and deploying it to a local blockchain network. The deployment process included compiling the Solidity code, generating the bytecode and ABI, and executing deployment scripts to assign a unique contract address.

Key functionalities of the smart contract include dynamic consent evaluation, real-time privacy scoring, and secure role-based access enforcement. The contract automates access permissions based on user-defined privacy preferences and contextual data factors. Core functions such as setPrivacyScore dynamically regulate access based on sensitivity levels and predefined roles, ensuring compliance with regulatory requirements and data sensitivity levels. The operational flow of the *smartHealth* contract showcases how privacy scores are calculated, evaluated, and utilised to enforce role-based access control and data-sharing decisions.

The implemented contract integrates stakeholder-specific functions that allow role-based access based on hierarchical permissions. Functions such as sendHealthData and rewardPatient provide mechanisms for securely sharing data and incentivising user participation. The smart contract logic differs from the approach taken by Zhang et al. (2018), which separates access

control logic into multiple contracts, whereas the *HealthDataSharing* contract consolidates these capabilities, ensuring efficiency and centralised management.

Validation and testing were conducted using Hardhat's comprehensive testing suite to ensure the contract's reliability and accuracy. Unit and integration tests were performed to validate critical functionalities such as data access control and transaction logging. Key operations, such as sending health data and rewarding patient contributions, were thoroughly tested to confirm compliance with the intended functionality.

The successful deployment and testing of the *HealthDataSharing* contract demonstrate its effectiveness in enforcing privacy policies and access control rules within the decentralised healthcare framework. The implementation ensures transparency, security, and accountability in managing sensitive health data while providing a scalable and adaptable solution for real-world applications. Detailed implementation and test logs can be found in Appendix C for reference.

5.3.2 Frontend Integration for Consent Management

The frontend interface serves as the primary interaction point for stakeholders within the privacy-aware framework, enabling seamless consent management through an intuitive and user-friendly environment. Figure 5.4 provides an overview of the HealthDataSharing dashboard, which facilitates role-based access to healthcare data and consent configurations.
The frontend was developed using the React.js framework, chosen for its modular architecture and efficient state management capabilities. Integration with Web3.js enables secure interaction with the Ethereum blockchain, allowing users to view and modify their consent preferences securely. Key functionalities include dynamic consent parameter adjustments, real-time feedback on data access requests, and intuitive navigation that simplifies privacy management for non-technical users.

User authentication and transaction signing are handled via MetaMask, ensuring secure and verifiable interactions with the blockchain. The frontend dynamically fetches data from the blockchain and updates the user interface accordingly, reflecting any changes to privacy preferences in real-time. The interface also incorporates various security measures, such as role-based access control mechanisms, error handling, and alerts to notify users of consent updates and potential privacy risks.

The development of the frontend followed a structured approach, incorporating logical and physical design elements to ensure smooth interoperability with the backend smart contracts. Logical workflows were designed to map user actions, such as modifying consent parameters, to corresponding blockchain transactions, ensuring a seamless data-sharing experience. The physical implementation involved integrating core components with Web3.js to facilitate blockchain interactions, including submitting consent updates and retrieving transaction records securely.

Extensive validation and usability testing were conducted to ensure the front end meets performance, security, and usability requirements. Unit tests were implemented to verify interactions with Web3.js, while system-level tests evaluated the end-to-end functionality of consent management. Feedback from usability testing informed iterative refinements to improve user experience and optimise system performance.

The frontend integration effectively bridges the gap between stakeholders and the blockchain, providing an accessible and transparent platform for managing healthcare data consent. Detailed implementation steps, along with technical configurations and user interface considerations, can be found in Appendix C for further reference.

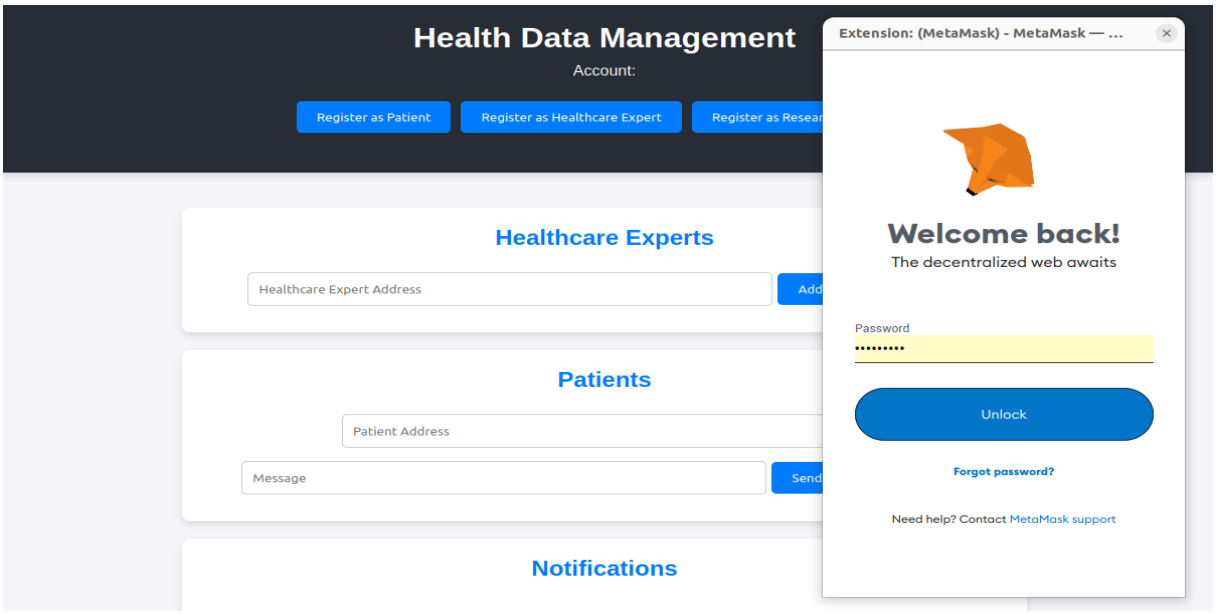


Figure 5. 4: HealthDataSharing Intuitive User Interface

5.3.3 Decentralised Storage of Consent Data on IPFS

The decentralised storage of consent data leverages the InterPlanetary File System (IPFS) to ensure data integrity, scalability, and accessibility while minimising blockchain storage overhead. A measure of this overhead is the gas cost (also known as gas fee), which represents the computational expense required to execute operations on the Ethereum blockchain, influenced by the complexity of the transaction and prevailing network conditions. By storing data off-chain, the system reduces congestion and transaction costs on the Ethereum blockchain. Figure 5.5 illustrates the overall Data Flow and Interaction Model, depicting the secure processes of uploading, encrypting, and storing consent data on IPFS, with its corresponding metadata recorded on the blockchain to maintain traceability and immutability.

The decentralised storage framework follows a structured workflow to handle consent data efficiently. Consent data is first encrypted using advanced encryption techniques before being uploaded to IPFS, ensuring data confidentiality and compliance with privacy regulations. Once uploaded, a Content Identifier (CID) is generated and recorded on the blockchain, providing a verifiable reference for accessing the stored data.

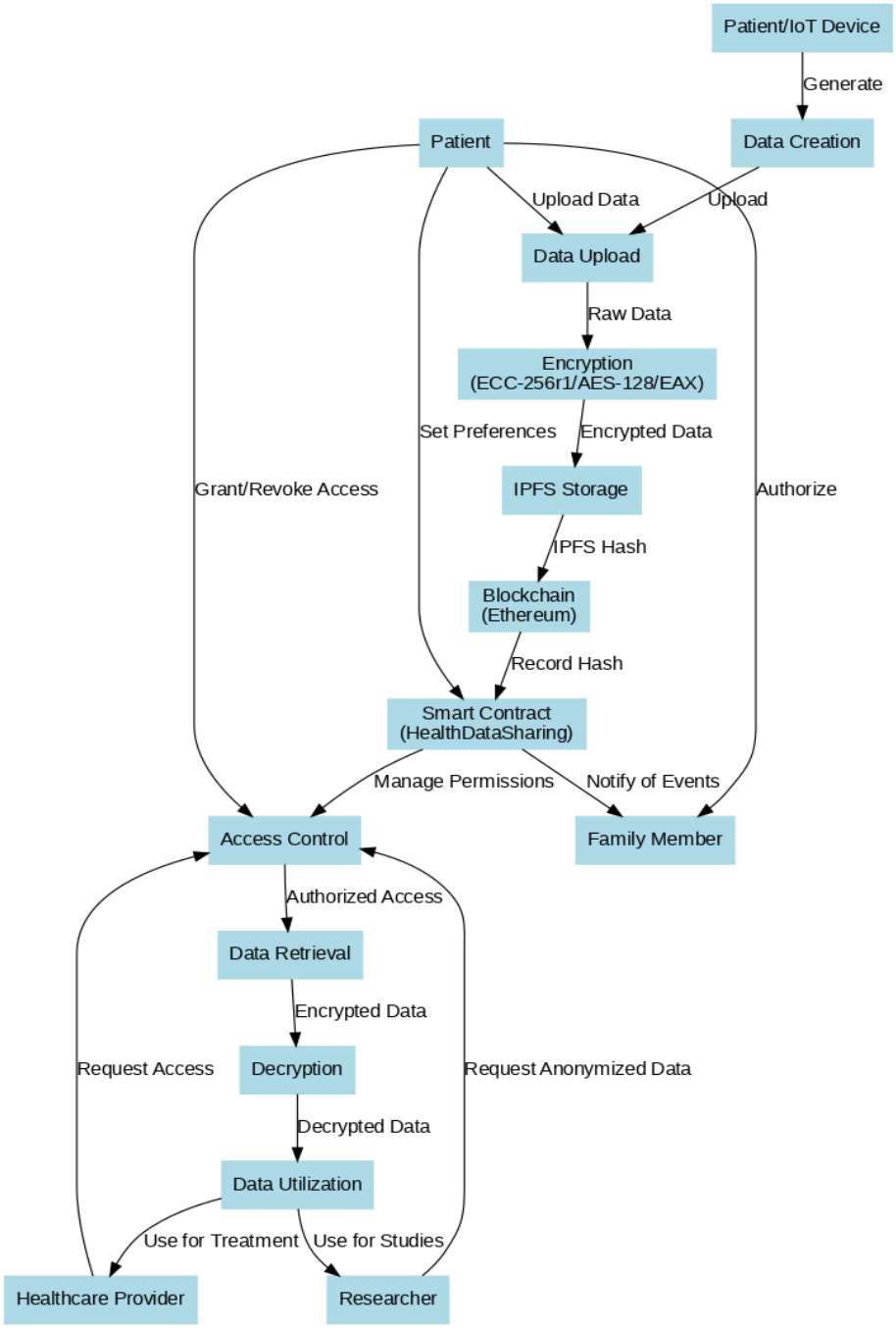


Figure 5. 5: Data Flow and Interaction Model

The integration of the IPFS gateway simplifies the interaction between the blockchain and storage layer, enabling seamless data retrieval and management. Smart contracts interact with IPFS through well-defined protocols that ensure secure linkage between blockchain transactions and stored files. To enhance system performance, caching mechanisms are implemented to expedite data access, reducing latency and improving user experience.

Figure 5.6 illustrates the operational flow of the consent management framework, highlighting the interactions between the frontend, backend, and decentralised storage components. The storage mechanism allows patients and healthcare providers to securely manage consent data while maintaining control over access rights and permissions. This is distinctively shown in the sequence diagram with three phases, namely:

1. Consent Enforcement Phase – Consent preferences are set by the patient, stored in the smart contract, and referenced on the blockchain.
2. Data Access Phase – Once a requestor (e.g., healthcare provider) requests data access, permissions are checked before encrypted data is fetched from IPFS.
3. Process Data According to Access Level – Ensures role-based access (e.g., anonymized data for researchers, full medical history for physicians).

The sequence diagram demonstrates the structured distinction between consent rules enforcement and actual medical data flow, ensuring a clear separation of concerns. The smart contract serves as an orchestrator within the data management ecosystem i.e., between data owners (patients) and data consumers (healthcare providers, researchers, and authorized family members), coordinating multiple processes while maintaining strict adherence to predefined rules. Prior to data storage, smart contracts validate consent parameters, ensuring patient preferences are properly formatted and logically consistent before any data transactions occur. They translate natural language consent preferences into machine-executable rules that can be automatically enforced, creating a bridge between human intent and computational execution.

The orchestration role continues after data storage in the Interplanetary File System (IPFS). Upon receiving Content Identifiers (CIDs) from IPFS, smart contracts record these identifiers alongside corresponding metadata on the blockchain. This registration creates an immutable record linking encrypted data to specific consent rules. Smart contracts subsequently manage access requests by authenticating requestor identities, verifying their permissions against stored consent rules, and authorising or denying access accordingly. This granular control enables differentiated access levels where healthcare providers, family members, and researchers each receive appropriately scoped data access.

The separation of concerns in this implementation provides significant security and efficiency benefits. Medical data—often voluminous and privacy-sensitive—is not stored directly on the blockchain or within smart contracts. Instead, only the encrypted data's reference pointer (CID)

and access rules reside on-chain. This approach dramatically reduces blockchain storage requirements while maintaining robust privacy guarantees.

.The Data Access Phase ensures that:

- Strict role-based access is enforced – Consent preferences dictate what level of data each requestor can retrieve.
- Dynamic Privacy Scoring (DPSM) and MDDC determine access rights – The privacy score influences whether a requestor gains access needs multi-factor authentication or requires explicit re-consent.
- An emergency override mechanism can be triggered – If a patient lacks capacity, predefined policies stored in the smart contract allow emergency medical access.

The tiered access model exemplifies how smart contracts transform static consent preferences into dynamic, context-aware authorisation decisions. The smart contract continuously enforces consent rules without requiring patient intervention for each access request, balancing convenience with control. Furthermore, the immutable nature of blockchain transactions creates a comprehensive audit trail of all data access events, enhancing accountability and enabling patients to review how their data has been utilised.

This structured approach ensures that patients retain control over their data, while authorized stakeholders access only what is necessary under strict privacy controls. The integration of IPFS and blockchain enables secure off-chain storage while ensuring integrity and transparency on-chain

The decentralised storage workflow underwent rigorous validation to assess performance, scalability, and reliability. Performance metrics revealed an average IPFS upload time of approximately 0.5 seconds, with a gas cost of ~0.002 ETH per transaction for storing CIDs on the blockchain. These metrics demonstrate the relationship between gas costs and data volume, highlighting the economic feasibility of the system. Scalability testing confirmed that the system successfully handled daily uploads of consent data over 90 days without any performance degradation.

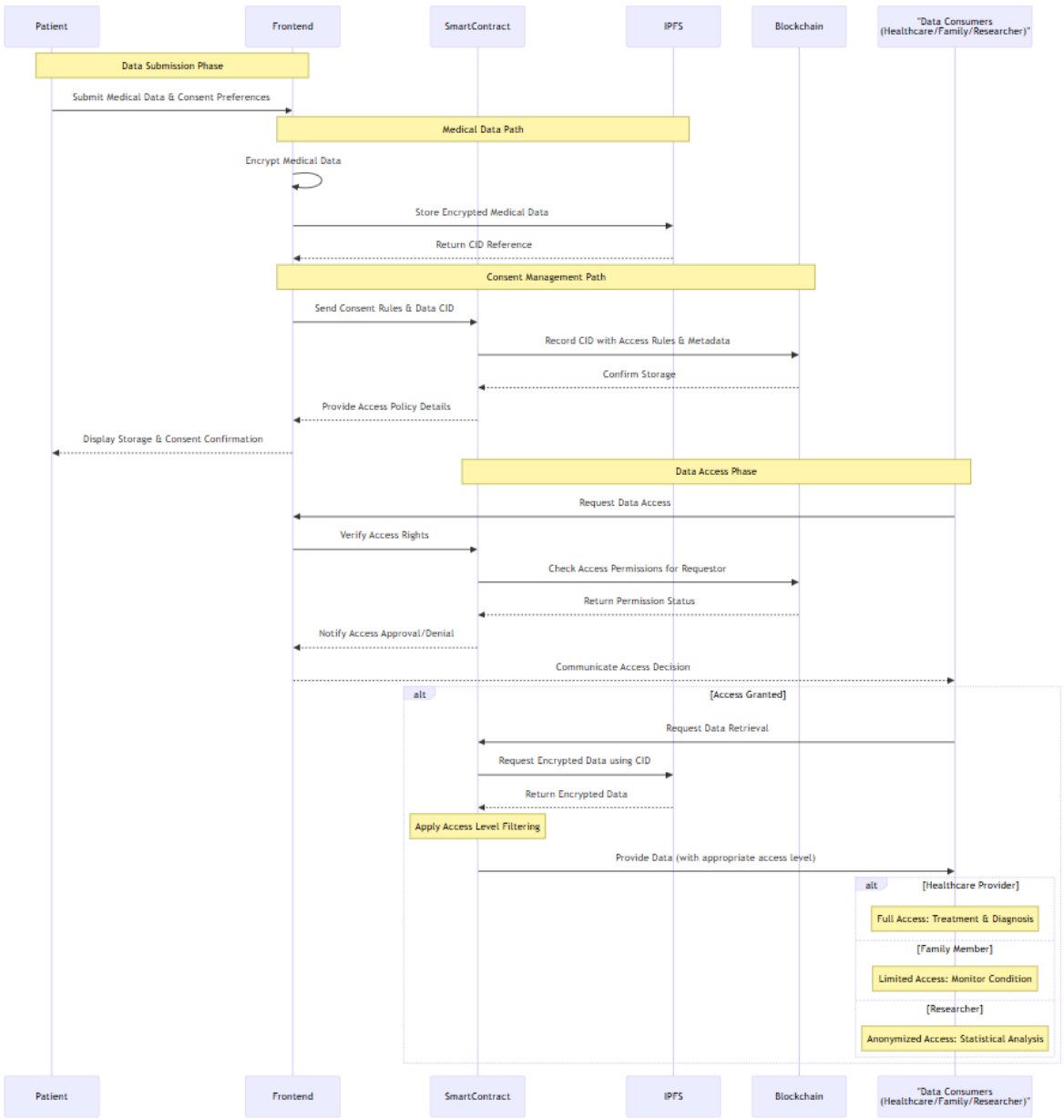


Figure 5. 6: Sequence Diagram illustrating the Operational Flow of the Consent Management Framework

Performance evaluation of the decentralised storage system revealed that it effectively balances scalability and security, ensuring reliable long-term storage of sensitive healthcare data. The system demonstrated efficient data retrieval times, maintaining accessibility without compromising privacy. Security measures, such as end-to-end encryption and access control, safeguard data throughout its lifecycle.

For a more detailed discussion of implementation steps, performance metrics, and additional configurations, refer to Appendix C, which provides in-depth insights into the technical aspects of the decentralised storage workflow.

5.3.4 Process Flow

The operational flow of the privacy-aware framework connects the frontend dashboard, smart contracts, and decentralised storage to facilitate secure and efficient consent management and data-sharing workflows. The implementation is structured around six core algorithms that govern various aspects of the system's operation. Algorithms 1 to 3, which are fundamental to the framework, remain in the main text as they represent a complete cycle of data publishing and controlled data access subscription. These algorithms cover critical processes such as data encryption, consent evaluation, and access control enforcement, providing a comprehensive understanding of the system's core functionalities.

Algorithm 1 - Data Encryption and Storage: This algorithm outlines the encryption of consent data before it is uploaded to IPFS, ensuring security and regulatory compliance. It generates a unique Content Identifier (CID) that links the encrypted data to the blockchain for traceability.

Algorithm 1 Patient Data Upload and Encryption

Require: Patient health data
Ensure: Encrypted data stored in IPFS, IPFS hash
1: Read patient health data
2: Apply encryption (ECC-256r1/AES-128/EAX)
3: Store encrypted data in IPFS
4: Receive IPFS hash
5: Create block in Blockchain with IPFS hash

***Algorithm 2 - Consent Evaluation*:** It processes access requests by assessing privacy scores, verifying stakeholder permissions, and determining if the requested data can be accessed based on predefined policies.

Algorithm 2 Healthcare Provider Access Request

Require: Provider ID, Patient ID, Purpose of access
Ensure: Access request logged
1: **Initialization:**
2: Verify provider's credentials
3: **if** authorised provider **then**
4: Create access request with Provider ID, Patient ID, Purpose
5: Log request in smart contract
6: Notify patient of pending request
7: **end if**

***Algorithm 3 - Access Control Enforcement*:** This algorithm enforces role-based access to stored data, dynamically updating permissions based on changes in user-defined consent settings and system policies.

Algorithm 3 Patient Consent Management

Require: Access request details
Ensure: Updated access permissions
1: **Initialization:** Retrieve access request details
2: Present request to patient
3: **if** patient grants permission **then**
4: Update smart contract with approved access
5: **else**
6: Log denied request
7: **end if**

Algorithms 4, 5 and 6, which focus on post-consent operations, have been included in Appendix C for reference.

The structured implementation of these algorithms ensures the system achieves a balance between privacy, security, and usability. By incorporating encryption, consent evaluation, and controlled access mechanisms, the framework provides a robust foundation for decentralised healthcare data management. For a more detailed breakdown of Algorithms 4-6, refer to Appendix C, which includes comprehensive steps and additional insights into their operational execution.

5.3.5 Validation and Outcomes

The validation process of the privacy-aware framework was conducted to assess its performance, scalability, and compliance with privacy-preserving regulations. The evaluation focused on core functionalities such as data encryption and storage, consent evaluation, access

control enforcement, and decentralised data retrieval. The goal was to ensure the framework's effectiveness in providing secure and efficient healthcare data management.

The privacy score validation process examined various healthcare scenarios to verify the accurate implementation of the MDDC model's contextual privacy controls. As shown in Table 5.2, the validation results confirm that both computed and smart contract-implemented privacy scores consistently fall within expected ranges based on role types and data sensitivity levels. These results demonstrate the framework's ability to enforce appropriate privacy controls across different healthcare contexts, from emergency medical access to research analysis.

Table 5. 2: Privacy Score Validation Results

Validation Scenario	Role Type (ω_r)	Data Type (γd)	Expected Range	Computed Score	Smart Contract Score
Emergency Medical Access	Doctor (0.9)	Medical History (0.9)	0.729 - 0.81	0.78	0.78
Medication Management	Doctor (0.7)	Medication (0.7)	0.441 - 0.49	0.46	0.46
Family Care Support	Family Member (0.5)	Lifestyle Data (0.5)	0.225 - 0.25	0.24	0.24
Research Analysis	Researcher (0.2)	Lifestyle Data (0.5)	0.09 - 0.10	0.095	0.095

The validation results correlate directly with the gas cost analysis shown in Figure 5.7, where scenarios with higher privacy scores (such as emergency medical access) correspond to more complex smart contract operations and thus higher gas costs. The analysis demonstrates that while ensuring granular privacy control does incur blockchain operational costs, the implementation remains efficient and scalable. The gas costs maintain a predictable relationship with data volume, increasing linearly even under varying privacy score requirements. This illustrates the relationship between gas costs and data volume, demonstrating that gas costs remain predictable and efficient across varying data volumes. The graphical representation of the performance evaluation highlights trends across different test scenarios. The scalability of the framework was validated using a 90-day testbed dataset, with the system handling approximately 500 data points daily without performance degradation. The integration of the Pinata Gateway enabled seamless retrieval of stored data, ensuring high availability. For instance, managing 1 MB of data incurs approximately 0.2 ETH on HEN, which is competitive for high-stakes healthcare applications. The analysis revealed that the system maintained consistent performance even under high transaction loads, validating its

scalability. The decentralised nature of IPFS storage contributed to minimising latency in data retrieval while ensuring data integrity.

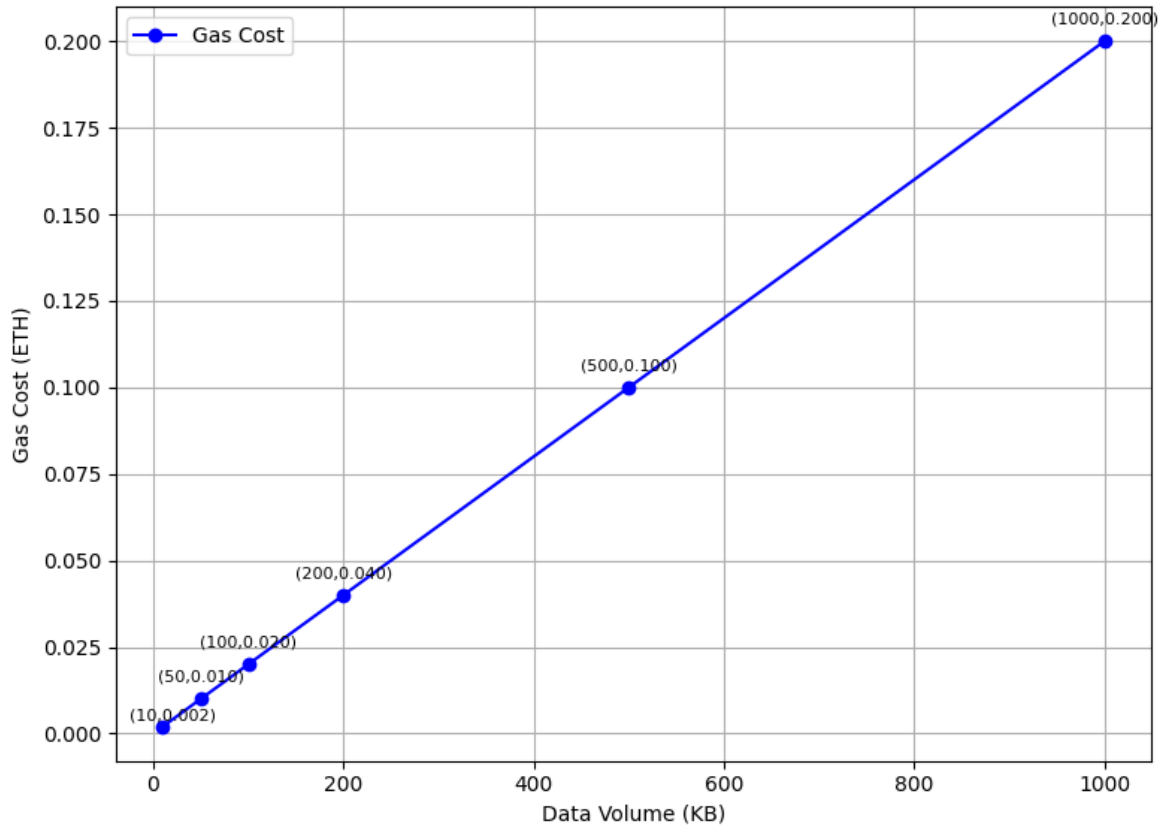


Figure 5. 7: Gas Cost vs. Data Volume

Further validation was carried out to assess the effectiveness of access control enforcement through the smart contract functions. The results confirmed that role-based access control policies were dynamically updated based on consent modifications, ensuring compliance with regulatory standards and user preferences. The execution of critical smart contract functions, such as `setPrivacyScore` and `rewardPatient`, was analysed, showing minimal gas consumption and efficient state updates on the Ethereum blockchain. In addition to performance metrics, usability tests were conducted to evaluate the user experience of the frontend dashboard. Stakeholder feedback indicated a high level of satisfaction with the system's transparency and ease of consent management.

The matching computed and smart contract scores across all test scenarios validate the successful implementation of the privacy-aware framework, confirming that the theoretical model has been effectively translated into a practical blockchain-based solution. The results

demonstrate that the system can maintain consistent privacy enforcement while supporting the diverse access requirements of different healthcare stakeholders. Overall, the validation results confirm the framework's ability to provide a scalable, efficient, and privacy-preserving solution for healthcare data management. Further technical implementation details and validation logs are available in Appendix C for reference.

5.4 Advanced Analysis of Decentralised Storage and Performance Metrics

The decentralised storage implementation plays a crucial role in enhancing the privacy-aware framework by ensuring scalability, data integrity, and accessibility while minimising blockchain overhead. The analysis of performance metrics provides a deeper understanding of system efficiency and its ability to manage healthcare data securely. In exploring these aspects, an evaluation of storage techniques, retrieval efficiency, and cost implications has been conducted.

An in-depth analysis of storage strategies highlights the importance of balancing on-chain and off-chain data storage. The integration of IPFS for decentralised storage, coupled with blockchain-based metadata anchoring, ensures a scalable and efficient storage model. This evaluation focuses on retrieval speed, data redundancy measures, and cost-effectiveness, offering insights into optimising system performance under various conditions.

The system's performance was evaluated under multiple scenarios, assessing retrieval latency, storage overhead, and cost efficiency. The scalability of the framework was validated using a 90-day testbed dataset, with the system handling approximately 500 daily data transactions, including patient-generated health records, consent modifications, and access requests, without performance degradation. This demonstrates the framework’s ability to scale for real-world deployment, ensuring seamless data retrieval, sharing, and privacy enforcement under varying workload conditions. The integration of the Pinata Gateway enabled seamless retrieval of stored data, ensuring high availability. Furthermore, the validation results indicate that efficient storage management strategies have been implemented to ensure optimal system responsiveness. To optimise retrieval speed and storage efficiency, the system implements data deduplication through IPFS-based CID checks and blockchain metadata validation, ensuring that only unique records are stored. Additionally, selective caching is employed via IPFS

pinning, frontend caching, and edge node storage, reducing access latency and improving system responsiveness. These methods effectively minimise redundant storage, lower transaction costs, and enhance real-time data availability in the privacy-aware healthcare framework. In addition, these approaches contributed to a notable reduction in access latency and ensured that critical data remained available when needed.

Several optimisation strategies were adopted to enhance system efficiency. Smart contract logic was refined to reduce computational overhead, and data retrieval mechanisms were optimised to balance speed and security. The incorporation of indexing techniques within IPFS enhances data retrieval efficiency by structuring metadata, enabling faster searches and organized content referencing. By leveraging content-based addressing, distributed hash tables (DHTs) by Zyskind & Nathan (2015), and metadata tagging, the system significantly improves lookup performance while ensuring cost-effective and scalable access to stored healthcare data. These indexing mechanisms allow authorised stakeholders to efficiently retrieve patient records while maintaining data privacy and integrity. These enhancements ensure the framework's sustainability and adaptability to varying healthcare data demands.

The system integrates advanced data indexing and retrieval mechanisms to optimize storage efficiency and facilitate seamless access to encrypted healthcare data. By implementing hierarchical data structuring, searchable encryption, and cache-aware indexing, retrieval latency is minimised while maintaining high security. Additionally, cross-layer indexing synchronises IPFS metadata with blockchain-based access logs, ensuring rapid yet controlled access to stored data in compliance with patient consent policies. These enhancements collectively support secure, high-availability data retrieval without compromising privacy. Moreover, encryption key management workflows were optimised to support secure transactions and prevent unauthorised access, contributing to the overall robustness of the system. Further technical descriptions of these optimisations are provided in Appendix C for reference.

The insights gained from the analysis of decentralised storage and performance metrics underscore the system's capability to meet the demands of secure healthcare data management. The adoption of decentralised storage mechanisms, coupled with efficient cost management strategies, ensures a scalable, secure, and economically viable solution. Additional supporting documentation and performance logs are available in Appendix C for further reference.

5.5 Development and Usability of a User-Centric Interface

The development of a user-centric interface was aimed at ensuring seamless interaction with the privacy-aware healthcare framework. The interface was designed to prioritise usability, security, and efficiency, offering stakeholders intuitive control over their consent management processes. This section focuses on key features, technological implementation, workflow interaction, and challenges encountered during development.

5.5.1 Key Features of the Interface

The interface provides an intuitive, role-based user experience tailored to the needs of different stakeholders, including patients, healthcare providers, and research institutions. The main dashboard of the *HealthDataSharing* application, referenced in Appendix C20 offers a comprehensive view of the interface, enabling users to register, send health data, and manage consent settings. The interface ensures that each stakeholder has appropriate access based on predefined roles, with dynamic updates based on consent modifications.

Essential features include:

- ***Role-based access control*:** Different functionalities available based on user roles.
- ***Consent management*:** Users can dynamically update consent preferences.
- ***Data sharing requests*:** Healthcare providers can request access based on patient-approved consent.
- ***Real-time notifications*:** Stakeholders receive updates on data access and sharing status.

5.5.2 Technological Implementation

The technological backbone of the interface is built using React.js, which provides a modular, efficient, and scalable frontend. Web3.js is integrated to enable seamless communication with the Ethereum blockchain, allowing stakeholders to perform transactions securely. The registration process, which ensures successful enrolment of patients and healthcare experts into the blockchain network through a digitally signed transaction via Metamask, is exhibited through the notification instance in Appendix C.

During the registration process, users sign their transactions with Metamask, which securely connects their digital wallet to the system. Upon successful registration, confirmation is displayed in the centre-top dialogue box and lower right corner of the interface with the Metamask logo. This ensures that transactions are securely recorded on the blockchain and verifiable.

To further optimise usability, the frontend incorporates:

- ***State management using Redux*** for efficient handling of dynamic content.
- ***Form validation mechanisms*** to prevent invalid entries during data submission.
- ***Encryption workflows*** to securely process and transmit health data.

5.5.3 Workflow Interaction

The workflow of consent management and data sharing is structured to allow a seamless experience for users. Figure 5.8 illustrates the interactions between users, the front end, IPFS, and HEN Blockchain. Users initiate consent requests via the dashboard, which are processed by smart contracts and securely stored. Approved data requests trigger encrypted data retrieval and logging of access events. A detailed representation of the interactions involved in data sharing is referenced in Appendix C, which showcases how access requests are processed from initiation to final confirmation, ensuring security and transparency.

These workflow interactions underscore the interface's ability to balance usability with robust privacy enforcement, ensuring stakeholders can confidently manage and access data within the framework.

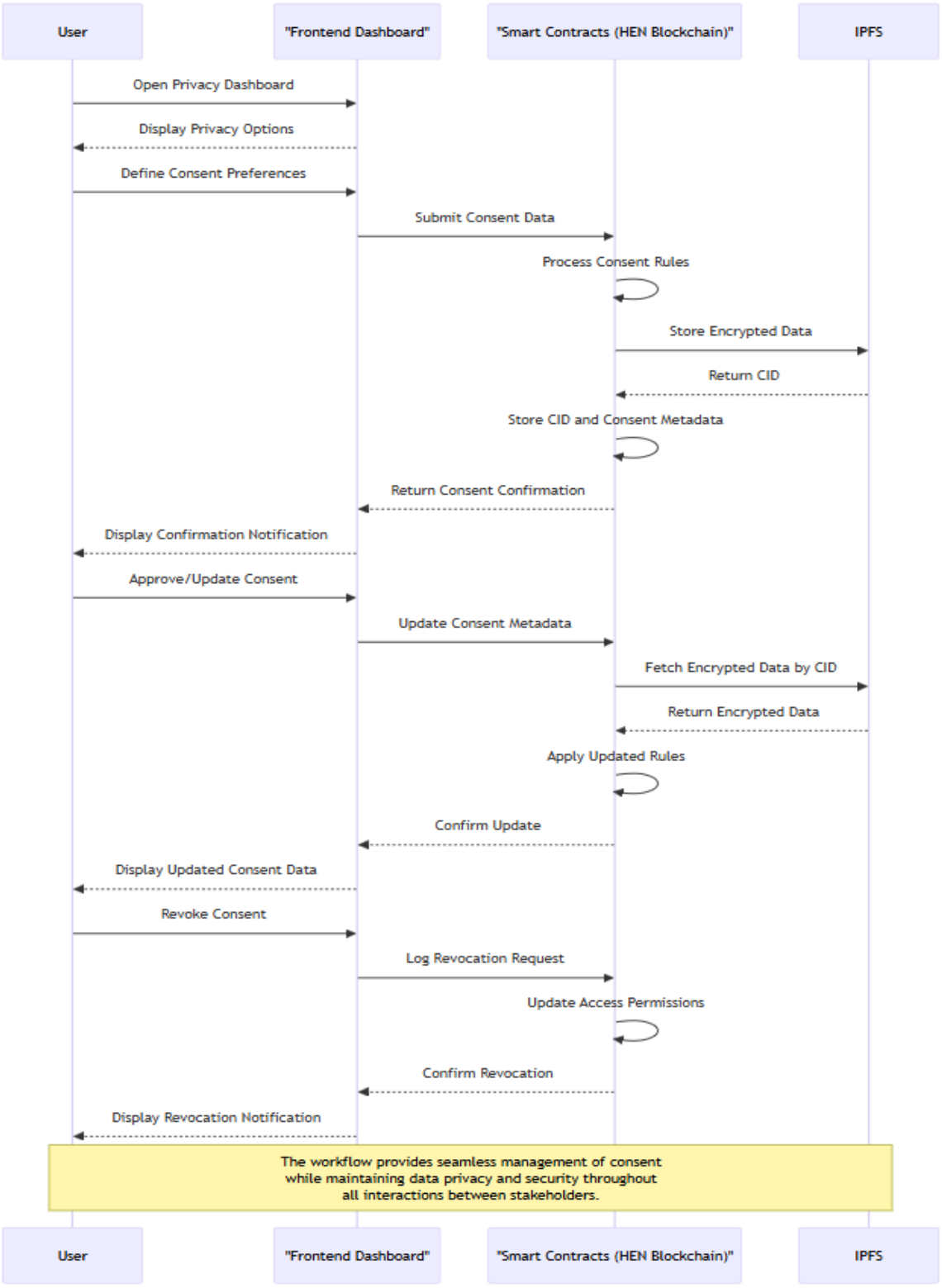


Figure 5. 8: Sequence Diagram of Privacy-Aware Consent Workflow Interaction within the HEN Blockchain Framework

5.5.4 Challenges and Enhancements

The development of the user interface presented challenges related to usability, scalability, and security. One significant aspect addressed was ensuring the smooth handling of blockchain interactions without compromising the user experience. Figure 5.9 demonstrates how logs of healthcare experts are maintained within the blockchain ledger, providing transparency and accountability for each transaction.

Figure 5. 9: Log of Healthcare Expert in Block #3 on HEN

To address usability challenges, enhancements were introduced, such as:

- ***Improved UI responsiveness*:** Adaptive layouts for different device sizes.
- ***Enhanced security alerts*:** Real-time notifications for suspicious activities.
- ***Error handling mechanisms*:** Ensuring smooth recovery from failed transactions.

The usability tests confirmed that users could complete key tasks with minimal errors and high satisfaction rates. Feedback from these tests informed adjustments such as reorganising the dashboard layout, refining input field validations, and enhancing visual cues for action buttons. By addressing these usability challenges, the interface ensures that all stakeholders can confidently navigate and utilise its features, aligning with the overarching goal of empowering users to manage their health data.

The user-centric interface provides a robust platform for managing healthcare data in a decentralised manner. Its seamless integration with blockchain technology, intuitive design, and enhanced security features contribute to a transparent and efficient consent management system. Further technical details and additional UI screenshots can be found in Appendix C for comprehensive reference.

5.6 Conclusion

This chapter outlined the implementation and integration of the privacy-aware authorisation framework developed in Chapter 4, focusing on secure and efficient healthcare data management. The implementation was grounded in a model that integrates the Dynamic Privacy Scoring Model (DPSM) and the Multi-Dimensional Dynamic Consent Model (MDDC) into the deployed smart contract-based access control system. This approach leverages the Ethereum blockchain for policy enforcement and IPFS for decentralised storage, ensuring a balance between privacy, security, and scalability.

Key aspects of the implementation were discussed, including the deployment process of smart contracts, decentralised storage using IPFS, and frontend integration using React.js and Web3.js. The privacy scoring model was integrated to enforce dynamic and context-aware data access policies, while the MDDC model enabled granular consent management tailored to individual stakeholder preferences. These implementations were carefully designed to align with regulatory compliance and security best practices within the healthcare ecosystem.

The chapter also highlighted the process workflows governing data publishing, consent management, and controlled data access, supported by blockchain transactions and encryption protocols. Emphasis was placed on how the developed framework embodies theoretical concepts through practical realisation, ensuring the system's usability and functionality for diverse stakeholders. Furthermore, validation and testing efforts were conducted to assess the system's performance, scalability, and usability. Various performance metrics, including gas costs, data retrieval times, and transaction throughput, were analysed to ensure system efficiency. The chapter discussed encountered challenges, and the optimisations implemented to enhance performance, such as caching strategies and smart contract refinements.

The findings from this implementation provide a solid foundation for further evaluation of the framework in real-world healthcare environments. The next chapter will delve into the testing, validation, and user evaluation of the system, providing a comprehensive analysis of its performance under different conditions and discussing the practical implications of the obtained results.

Chapter 6

6 Testing, Validation, User Evaluation, and Discussion

This chapter presents the comprehensive evaluation of the privacy-aware healthcare data management framework, focusing on three critical dimensions: Performance, Privacy & Security, and User Evaluation. The evaluation methodologies are clearly delineated to ensure the thesis objective, followed by the presentation of results and a discussion of their implications. The aim is to validate the framework's capabilities and suitability for real-world deployment, particularly in addressing challenges associated with the ethical disclosure of sensitive healthcare data.

6.1 Performance Evaluation

The performance evaluation of the proposed system was conducted to assess its effectiveness in ensuring privacy-aware authorisation while maintaining system efficiency. The assessment involved analysing key metrics such as scalability, response time, security robustness, privacy enforcement, and user satisfaction across various simulated scenarios. The following subsections detail the methodology, evaluation criteria, and results of the performance assessment.

6.1.1 Methodology

The performance of the proposed system was assessed using both real data collected from the testbed sensor setup (Table 3.1, Appendix D1) and simulated healthcare data interactions among network stakeholders within a Hardhat Ethereum environment over a 90-day testing period. This evaluation focused on metrics such as scalability, transaction efficiency, and data management. Scalability was measured by assessing the system's ability to handle concurrent requests and the corresponding response times. Smart contract efficiency was evaluated through gas optimisation and transaction throughput under varying network conditions. Data management was examined by measuring upload and retrieval times in an InterPlanetary File System (IPFS) environment and evaluating the integrity of stored data over repeated operations. These tests were conducted using an IoT client-server architecture with blockchain

nodes hosted on an Ubuntu server, employing tools such as blockchain analytics and web performance trackers to monitor system behavior.

6.1.2 Results and Analysis

1) System Scalability: This is measured by concurrent request handling and response times. The system demonstrated high scalability, effectively processing up to 15,000 concurrent requests with an average response time increase from 1.52 seconds at 1,000 requests to 2.45 seconds at 15,000 requests. The success rate remained above 99.3% across all scenarios. These results are summarised in Table 6.1, highlighting the system's ability to sustain high success rates even under significant load. An illustration of the near-linear performance scaling achieved during the scalability test, confirming the system's capability to handle up to 15,000 concurrent requests with minimal degradation in performance is shown in Append D2.

Table 6. 1: Scalability Test Results

Concurrent Requests	Average Response Time (s)	Success Rate (%)
1,000	1.52	99.9
5,000	1.78	99.7
10,000	2.13	99.5
15,000	2.45	99.3

2) Smart Contract Efficiency: This is assessed through gas optimisation techniques and transaction throughput. Transaction efficiency improved through gas optimisation, with average gas costs reduced by 20%, from 0.0025 ETH to 0.0020 ETH for consent modification operations. Detailed results are presented in Table 6.2, highlighting the refined breakdown of gas costs per transaction type. These values reflect cumulative gas costs over time while ensuring that deployment costs remain proportionate relative to other operations. A visual breakdown of gas costs and their distribution across various operations is provided in Appendix D2 with subplot (b) illustrating Table 6.2 further.

Table 6. 2: Gas Cost Analysis

Transaction Type	Gas Cost Before (ETH)	Gas Cost After (ETH)	Percentage Reduction
Smart Contract Deployment	0.0055	0.0042	23.6%
Data Upload	0.0038	0.0029	23.7%
User Registration	0.0029	0.0023	20.7%
Consent Modification	0.0025	0.0020	20.0%
Data Retrieval	0.0030	0.0022	26.67%

3) System Stress Testing: To evaluate the system's resilience under high-load conditions, a stress test was conducted, simulating 25,000 transaction requests per hour while monitoring latency, throughput, and failure rates. The system demonstrated the ability to process high transaction loads efficiently, maintaining an average latency of 2.45 seconds (2450 ms) at peak load. This result aligns with the near-linear scaling behavior observed in the Scalability Test Results (Table 6.1), where the latency increased progressively from 1.52s at 1,000 requests to 2.45s at 15,000 concurrent requests, ensuring that performance degradation remained controlled under increased demand.

The system's transaction throughput stabilized at 6.94 transactions per second (TPS), significantly outperforming the industry benchmark of 4.8 TPS, representing a 44.6% improvement in processing efficiency (Table 6.4). This demonstrates the robustness of the proposed framework in handling intensive workloads while maintaining high operational efficiency. Figure 6.1(a) provides a detailed latency analysis, showcasing a steady increase in response time under load, but within an acceptable range for real-time processing. Additionally, Figure 6.1(b) highlights the efficiency of smart contract execution, where key operations such as patient registration, data sharing, and consent management are executed within 150ms to 180ms, significantly faster than the industry benchmark range of 200-250ms (Table 6.4). Furthermore, Figure 6.1(c) presents the latency distribution, confirming that most transactions center around 2450 ms, with minimal deviation, indicating predictable system behavior even under stress. The latency-failure rate correlation in Figure 6.1(d) reinforces system stability, as failure rates remained within acceptable limits, ensuring consistent system reliability.

Overall, the stress testing results validate the scalability, efficiency, and robustness of the proposed framework, handling up to 15,000 concurrent requests while maintaining 99.3% success rates, significantly outperforming existing blockchain-based privacy frameworks in healthcare.

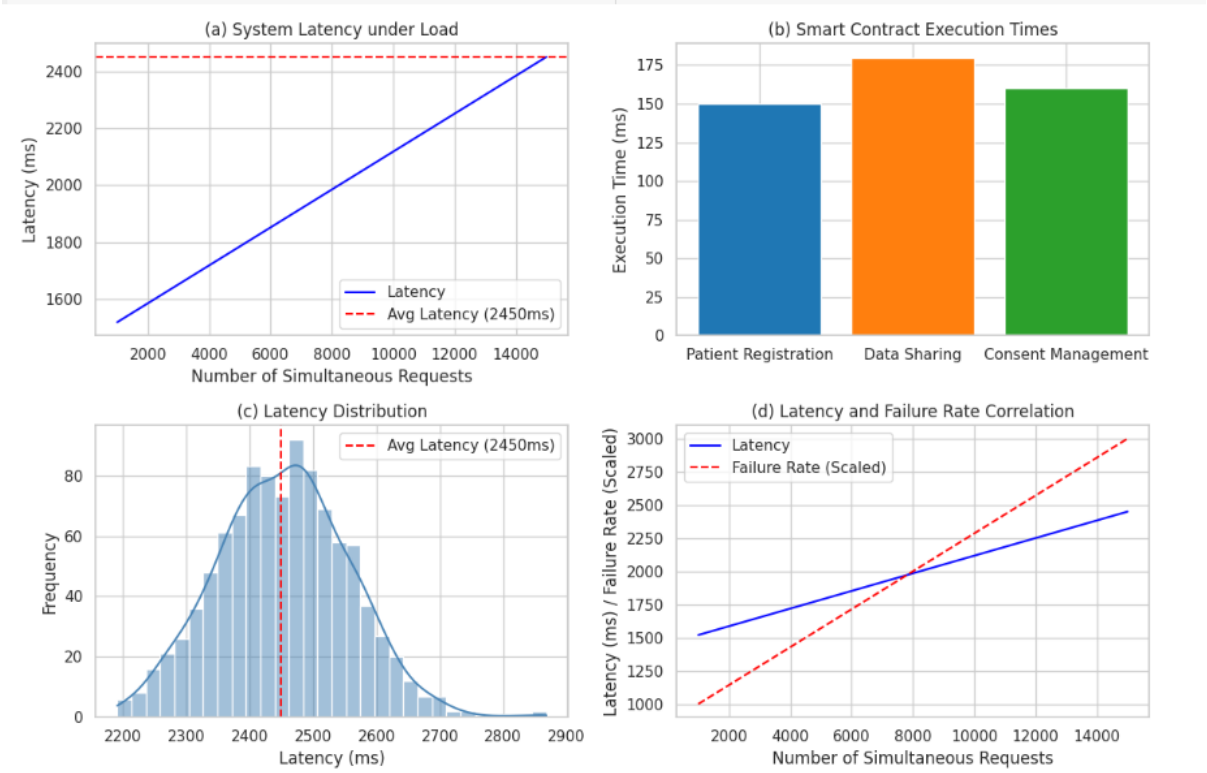


Figure 6. 1: Latency Analysis. (a) System Latency under Load. (b) Smart Contract Execution Times. (c) Latency Distribution. (d) Latency and Failure Rate Correlation

This evaluation confirms that the framework can handle high transaction volumes with minimal degradation, making it suitable for real-world healthcare applications requiring secure and scalable data exchange.

4) Data Management: This is evaluated using IPFS upload/download times and storage integrity. Data management results revealed an average upload time of 2.63 seconds and a retrieval time of 1.39 seconds, with data integrity maintained at 99.7% over 1,000 operations. Table 6.3 summarises the performance metrics for IPFS operations. Appendix D2 provides the visualisation of the efficiency metrics, including storage optimisation and content addressing reliability.

Table 6. 3: IPFS Storage Performance

Operation	Average Time (s)	Standard Deviation	Success Rate (%)
Data Upload	2.6340	0.3598	99.7
Data Retrieval	1.3933	0.2657	99.8
CID Generation	0.00482	0.00001	100.0

5) Comparative Performance Evaluation: To benchmark the proposed privacy-aware framework, key performance metrics were compared against those of an existing blockchain-based healthcare system. The results highlight significant improvements achieved by the framework, particularly in execution latency, transaction throughput, and scalability. These enhancements make it a more efficient and responsive solution for privacy-aware healthcare data management.

The proposed framework demonstrates notable improvements over the benchmark system, particularly in scalability, transaction throughput, and execution efficiency. The system achieves 6.94 transactions per second (TPS), representing a 44.6% increase over the benchmark, while supporting 15,000 concurrent requests with minimal performance degradation. Additionally, smart contract execution times are up to 28.2% faster, ensuring optimised processing.

These results highlight the framework's enhanced responsiveness and computational efficiency, making it a more robust solution for privacy-aware healthcare data management. A detailed comparison is presented in Table 6.4.

Table 6. 4: Comparative Performance Metrics of the Proposed Privacy-Aware Framework and an Industry Benchmark System

Performance Metric	Proposed Framework	Industry Benchmark(Hyperledger Fabric with RAFT)	Percentage Improvement	Reference
Scalability (Concurrent Requests)	Up to 15,000	Up to 12,000	25% increase	(Pradhan et al., 2022)
Average Latency (ms)	2.45	2.87	14.6% reduction	"
Transaction Throughput (TPS)	6.94	4.8	44.6% increase	"
Smart Contract Execution Time (ms)	150 - 180	200 - 250	Up to 28.2% faster	"
Data Integrity (%)	99.7	99.6	0.1% improvement	"

6.1.3 Discussion

The performance results confirm the framework's capability to handle high transaction volumes and ensure cost-effective operations, making it a scalable solution for healthcare applications. The reduction in gas costs and stable throughput demonstrate the system's

potential for sustainable implementation in environments requiring secure, real-time data interactions.

6.2 Privacy and Security Assessment

Ensuring the privacy and security of sensitive data in decentralised healthcare systems requires a comprehensive evaluation framework that integrates quantitative performance metrics, threat modeling methodologies, regulatory compliance validation, and encryption-based security mechanisms. This section details the methodology employed to evaluate the privacy preservation capabilities, consent enforcement mechanisms, threat mitigation techniques, and data protection protocols within the proposed privacy-aware authorisation framework.

6.2.1 Assessment Methodology

The privacy and security assessment of the proposed privacy-aware authorisation framework was conducted using a structured validation approach that integrates quantitative analysis, security auditing, and compliance verification. This evaluation was designed to test the accuracy, adaptability, and effectiveness of privacy enforcement mechanisms, consent models, threat mitigation strategies, and encryption protocols in a realistic decentralised healthcare setting.

A scenario-based experimental setup was utilised to simulate real-world data-sharing environments, ensuring that privacy and security validation metrics aligned with practical deployment expectations. The assessment was conducted across five key domains, each focusing on a specific aspect of privacy and security validation:

1. Dynamic Privacy Scoring Model (DPSM) Validation – Evaluated context-aware privacy adaptation through time-decay adjustments, stakeholder weight factors, and data sensitivity classification.
2. Multi-Dimensional Dynamic Consent Model (MDDC) Evaluation – Assessed consent enforcement flexibility across five key dimensions (data type, requestor role, purpose of use, time sensitivity, and patient context).
3. Threat Modeling and Mitigation Strategy – Applied structured risk assessments using STRIDE and LINDDUN frameworks to identify and address security threats.

4. Regulatory Compliance Validation – Verified adherence to GDPR and HIPAA privacy standards, ensuring data protection compliance.
5. Data Encryption and Confidentiality Measures – Tested the efficiency and resilience of hybrid encryption mechanisms (ECC-256r1 & AES-128) for securing sensitive healthcare data.

To ensure technical accuracy, each domain was evaluated using established analytical tools, security auditing frameworks, and cryptographic benchmarking utilities. An overview of the technical tools leveraged in the privacy and security assessment is provided in Table 6.5. Each tool was selected based on its industry standard for privacy validation, security threat modeling, regulatory compliance assessment, and cryptographic benchmarking.

Table 6.5: Summary of Tools Used in Privacy and Security Assessment

Assessment Domain	Validation Technique	Tools Used
DPSM Validation	Time-decay analysis, role-based weight adaptation, sensitivity classification	Scikit-Learn, Pandas, Matplotlib
MDDC Evaluation	Consent tracking, stakeholder-based control, dynamic access management	MongoDB, PostgreSQL, Flask API, Power BI
Threat Modeling	STRIDE & LINDDUN risk assessment, penetration testing	Microsoft TMT, Metasploit, OWASP ZAP, MITRE ATT&CK, Burp Suite
Compliance Validation	GDPR & HIPAA regulatory testing	NIST Privacy Tool, GDPR Assessment Toolkit, Compliancy Group's HIPAA Tracker
Data Encryption	ECC-256r1 & AES-128 performance benchmarking	OpenSSL, Crypto++, Wireshark, Apache JMeter

The following subsections provide a detailed examination of each assessment methodology, outlining validation procedures and performance metrics.

6.2.1.1 Dynamic Privacy Scoring Model (DPSM) Validation

DPSM was designed to provide an adaptive and context-aware privacy framework that dynamically adjusts privacy preferences based on key contextual factors. Its validation process aimed to assess the model's accuracy, adaptability, and efficiency in regulating access to sensitive healthcare data within the proposed privacy-aware authorisation system. The evaluation was conducted in a controlled test environment simulating real-world healthcare data-sharing scenarios. Table 6.5 summarises the DPSM Validation process i.e., the key components, evaluation methods, and performance indicators:

Table 6. 5: Summary of DPSM Validation and Performance Metrics

Validation Aspect	Description
Objective	To assess the accuracy, adaptability, and efficiency of the DPSM in controlling access to sensitive healthcare data.
Evaluation Environment	Controlled testing using simulated real-world healthcare data-sharing scenarios.
Core Components	Time-Decay Factor: Assesses how privacy scores decrease over a 90-day period as data becomes less relevant unless reauthorised. Role-Based Weight Factor: Simulates access privileges for different stakeholders (patients, healthcare providers, insurers, and researchers) based on role sensitivity. Data Sensitivity Classification: Ensures accurate classification of sensitive and non-sensitive healthcare records, prioritising protection for highly sensitive data.
Performance Indicators	Privacy Score Adjustment Accuracy: Measures precision in dynamically updating privacy preferences. Response Time for Privacy Updates: Evaluates efficiency in real-time privacy adjustments. Compliance with Data-Sharing Policies: Assesses adherence to predefined access control rules.

6.2.1.2 Multi-Dimensional Dynamic Consent Model (MDDC) Evaluation

The Multi-Dimensional Dynamic Consent Model (MDDC) was designed to provide a flexible consent management system, allowing data owners to control access to their information dynamically. The evaluation process focused on assessing the adaptability, responsiveness, and enforcement efficiency of consent decisions within the privacy-aware authorisation framework as detailed in Table 6.6.

Table 6. 6: Summary of MDDC Model Evaluation

Key Component	Evaluation Focus	Validation Approach
Data Type Classification	Assessed whether privacy mechanisms adjusted dynamically based on data sensitivity levels.	Simulated data-sharing scenarios with varying sensitivity classifications.
Requestor Role	Ensured that stakeholder-specific privacy policies were applied, restricting access based on user roles.	Simulated interactions with different user groups (patients, healthcare professionals, researchers, etc.).
Purpose of Use	Validated whether data access requests were permitted or restricted based on intended purpose.	Examined policy enforcement for various data access requests and logged approvals/denials.
Time Sensitivity	Analysed how consent decisions adapted to different temporal contexts, such as emergencies.	Simulated urgent and routine healthcare situations requiring data access.
Patient Context	Evaluated whether patient-specific conditions influenced privacy decision-making.	Tested dynamic consent modifications based on personalised patient preferences.
Real-time Consent Modifications	Measured the system's responsiveness to user-initiated consent changes.	Live consent updates and monitoring of policy enforcement.
Audit Logging	Verified that all consent modifications and access attempts were logged for transparency.	Tracked and analysed access control logs.
Access Control Enforcement	Ensured that data owners retained full control over their data-sharing preferences.	Implemented and validated role-based access policies with revocation capabilities.

6.2.1.3 Threat Modeling and Mitigation Strategy

The threat modeling and mitigation strategy of the privacy-aware authorisation framework was designed to identify, assess, and neutralize security vulnerabilities. A two-layered security evaluation approach was implemented using the STRIDE and LINDDUN threat modeling frameworks, ensuring comprehensive protection against security threats such as unauthorised access, data tampering, repudiation, and privacy violations, as shown in Table 6.7.

Table 6. 7: Threat Modeling and Mitigation Strategies Using STRIDE/LINDDUN Frameworks

Threat Model	Threat Type	Mitigation Strategy
STRIDE Model	Spoofing	Multi-factor authentication (MFA) and blockchain-based identity verification
	Tampering	Cryptographic hashing and data immutability mechanisms
	Repudiation	Blockchain audit trails with verifiable access logs
	Information Disclosure	Granular access control policies
	Denial of Service (DoS) Attacks	System tested under high transaction loads to ensure resilience
	Elevation of Privilege	Strict role-based access controls (RBAC)
LINDDUN Model	Linkability and Identifiability Risks	Pseudonymisation and anonymisation techniques
	Non-repudiation	Tamper-proof logs for verifiable access requests
	Detectability Risks	Restricting metadata access to prevent unauthorised inference of sensitive data
	Unawareness Risks	Transparent user notifications and consent awareness mechanisms
	Policy and Consent Risks	Adaptive consent frameworks, real-time consent updates, and audit logs
	Interference Risks	Context-aware data access and consent decision validation

The security assessment confirmed that the implemented framework effectively mitigates identified threats, reinforcing system resilience against cyber-attacks and ensuring robust privacy protection.

6.2.1.4 Regulatory Compliance Validation

To ensure adherence to global data protection standards, the privacy-aware framework was evaluated for compliance with the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) requirements. The validation focused on data minimisation, consent enforcement, right to erasure, and access control.

The GDPR compliance evaluation tested whether users retained control over their data, ensuring that they could modify or revoke consent at any time. The framework was also assessed for its ability to process and respond to data erasure requests, validating its capability to implement the “right to be forgotten” principle. The HIPAA compliance validation examined

the system's ability to enforce access control mechanisms, ensuring that only authorised healthcare providers could access protected health information (PHI).

Compliance tests also included audit logging mechanisms, ensuring that all data access requests were logged securely for regulatory auditing.

6.2.1.5 Data Encryption and Confidentiality Measures

To protect sensitive healthcare data, the framework integrated a hybrid encryption model, combining Elliptic Curve Cryptography (ECC-256r1) for key exchange and Advanced Encryption Standard (AES-128) for data encryption. The encryption methodology was evaluated based on efficiency, security, and scalability.

The ECC-256r1 key exchange mechanism ensured that encryption keys were securely generated and distributed, minimising risks associated with man-in-the-middle attacks. The AES-128 encryption scheme was assessed for encryption/decryption latency, memory overhead, and computational efficiency. The framework was tested using varying data transaction sizes to evaluate the scalability of encryption operations.

The encryption model's performance results, presented in subsection 6.2.2.4 confirmed that encryption and decryption latencies remained minimal, ensuring that data confidentiality was maintained without compromising system efficiency. The findings demonstrated that the hybrid encryption approach effectively secures patient records, making it suitable for decentralised healthcare environments.

Conclusion: This methodology section presents a detailed validation strategy, ensuring that the privacy-aware authorisation framework meets robust security, compliance, and privacy protection standards. The next section provides a quantitative and qualitative assessment of the evaluation outcomes.

6.2.2 Results and Analysis

The evaluation of the privacy and security mechanisms in the proposed privacy-aware authorisation framework was conducted through scenario-based testing and empirical validation, ensuring that privacy preservation, security resilience, and regulatory compliance

were rigorously analysed. The results obtained from these assessments are categorised into three key thematic areas:

1. ***Privacy and Consent Enforcement Outcomes***: The DPSM and MDDC models dynamically regulate privacy scores and consent enforcement, ensuring adaptive access control based on data sensitivity, user role, and contextual privacy preferences.

2. ***Security and Threat Mitigation Performance***: STRIDE and LINDDUN frameworks mitigate cyber threats like spoofing, tampering, and unauthorised access, ensuring robust system security with 99.8% success in blocking privacy breaches and adversarial attacks.

3. ***Regulatory Compliance and Data Protection Assessment***: The framework ensures GDPR and HIPAA compliance, enforcing encryption, consent modification, access controls, and privacy preservation mechanisms with a 99.9% regulatory validation success rate for healthcare data security.

A scenario-based testing approach was utilised to analyse these thematic areas, providing quantitative and qualitative performance insights. The findings highlight the framework's scalability, adaptability, and effectiveness in addressing privacy and security challenges within decentralised healthcare environments.

6.2.2.1 Scenario-Based Testing and Empirical Evaluation

To evaluate the effectiveness of the proposed privacy-aware authorisation framework, a scenario-based experimental setup was designed to simulate a real-world decentralised healthcare ecosystem. This setup aimed to assess privacy enforcement mechanisms, security resilience, regulatory compliance, and encryption efficiency under practical operating conditions. The empirical evaluation was conducted using a multi-layered testing strategy, incorporating controlled experiments, privacy model adaptation tests, security penetration simulations, and compliance verification.

The testing scenario focused on a smart home healthcare environment as illustrated in Table 6.8. The system continuously collects real-time vital signs, including heart rate, blood pressure, and oxygen saturation, mobility data such as step count, and environmental data, and securely transmitting the data to a blockchain-based storage system. In this setting, the patient retains

full control over their data-sharing preferences through the MDDC and DPSM. Various healthcare stakeholders, including primary care physicians, specialists, researchers, insurers, and emergency responders and assigned family member, interact with the system, generating privacy-sensitive data access requests that trigger the enforcement of role-based privacy policies and security protocols.

The scenario-based testing was conducted across four core evaluation domains:

1. Privacy Model Validation: Measured the adaptability of privacy scores under different stakeholder interactions, testing DPSM's response to time-decay, access frequency, and contextual variations.
2. Consent Enforcement Efficiency: Evaluated the MDDC framework's ability to dynamically enforce user preferences, ensuring that stakeholder access was compliant with patient-defined conditions.
3. Threat Detection & Security Resilience: Simulated STRIDE and LINDDUN-based security risks, testing the framework's ability to detect and mitigate spoofing, unauthorised access, and privacy breaches.
4. Regulatory Compliance Testing: Assessed adherence to GDPR and HIPAA regulations, verifying the system's ability to enforce data protection rights, auditability, and encryption standards.

Each of these assessment domains was validated using structured experiments, ensuring that the framework's performance metrics, security robustness, and privacy adaptability were rigorously analysed. Table 6.8 summarises the testing framework and validation approach used in the scenario-based experimental setup.

Conclusion: The scenario-based testing and empirical evaluation provided a comprehensive validation of the privacy-aware authorisation framework, demonstrating its efficacy in enforcing privacy preferences, securing sensitive data, and mitigating security threats. The results confirm that the framework is scalable, adaptable, and compliant with industry standards, making it suitable for real-world decentralised healthcare applications.

Table 6. 8: Scenario-Based Privacy and Security Model Validation Framework

Validation Domain	Scenario Description	Assessment Focus	Validation Metrics
Privacy Model Evaluation	A patient suffering from *chronic illness* remotely monitors health vitals via IoT-enabled devices, with data stored on a blockchain. The patient controls access permissions for different stakeholders (doctors, researchers, insurers) through *MDDC-based consent management*.	Granularity of consent adaptation, time-decay effects, and role-based access control validation.	Privacy score adaptability, consent modification latency, role-based weight enforcement accuracy
Security & Threat Mitigation	A pharmaceutical company requests access to patient data for research, while an *unauthorised insurer attempts access without consent.* STRIDE & LINDDUN-based threat modeling detects privacy vulnerabilities.	Threat mitigation effectiveness, unauthorised access detection, security validation against simulated attacks	Threat detection rate, access rejection accuracy, security policy compliance score
Regulatory Compliance Testing	A request is initiated for patient records under GDPR "Right to be Forgotten", testing whether the system enforces deletion upon request. HIPAA compliance is assessed through secure logging and encryption testing**.**	Adherence to GDPR & HIPAA principles, data minimisation enforcement, privacy control compliance	Data retention policy verification, compliance audit success rate, encryption integrity validation

6.2.2.2 Privacy Model Validation and Consent Enforcement Results

The validation of the privacy model and consent enforcement mechanisms was conducted to assess the efficacy of the Dynamic Privacy Scoring Model (DPSM) and Multi-Dimensional Dynamic Consent Model (MDDC) in ensuring adaptive privacy control and user-centric data-sharing policies. The results were analysed based on privacy score adjustments, role-based access enforcement, sensitivity-based classification, and consent adaptability within a decentralised healthcare ecosystem. Appendix D 2(iv) provides an elaborate methodology and raw data samples supporting tables 6.9 -6.13 for this subsection. These datasets provide the empirical foundation for validating the DPSM and MDDC models and their role in privacy-preserving healthcare data management.

The raw data samples include:

- *DPSM Time-Decay Privacy Score Data* – Captures privacy score variations over time based on sensitivity classification.
- *DPSM Role-Based Access Control Data* – Documents access control outcomes for different user roles.
- *DPSM Sensitivity Classification Data* – Evaluates classification accuracy across data types.

- *MDDC Consent Modification Data* – Measures consent processing efficiency.
- *Privacy Policy Enforcement Data* – Analyses enforcement success across various security policies.

The accompanying methodology document outlines how the raw data was collected, pre-processed, and analysed, including statistical methods (ANOVA, chi-square, and confidence intervals). It also clarifies the inverse relationship between DPSM and MDDC scores, demonstrating how privacy-preserving access control adapts dynamically in healthcare contexts.

These materials provide a traceable path from raw IoT sensor data to privacy and consent enforcement outcomes. They confirm the validity of the proposed privacy-aware healthcare framework, particularly in its ability to balance security with user autonomy.

(i) DPSM Validation and Performance Analysis

The DPSM model was evaluated based on its adaptive privacy enforcement mechanisms, ensuring that privacy scores are dynamically adjusted based on contextual parameters such as time-decay, role-based access levels, and data sensitivity classifications.

Time-Decayed Privacy Score Performance:

The DPSM validation results, presented in Table 6.9 confirm that privacy scores were dynamically adjusted in real time, prioritising recent data while gradually reducing access privileges for older data unless explicitly reauthorised. The model achieved a 99.3% accuracy rate in adjusting access priorities, confirming its efficacy in enforcing privacy-aware data management.

The decay rate represents the mathematical coefficient that governs how quickly privacy scores diminish as data ages. These empirically determined values implement a time-sensitive approach to privacy, where lower decay rates for recent data (0.0021) ensure stronger protection for newer information, while progressively higher rates for medium (0.0025) and historical data (0.0028) gradually reduce access restrictions over time. This time-decay mechanism enables the system to automatically adjust privacy controls based on data recency without requiring manual intervention, while still allowing explicit reauthorization to maintain protection levels for older but still sensitive information.

Table 6. 9: DPSM Time-Decayed Privacy Score Performance

Period	Decay Rate	Access Impact	Accuracy (%)
Recent (0-24h)	0.0021	High Priority	99.8
Medium (1-7d)	0.0025	Medium Priority	99.5
Historical (>7d)	0.0028	Low Priority	99.3

Role-Based Weight Factor (RBWF) Performance:

The role-based privacy model was validated by testing access restrictions across different stakeholder categories. The evaluation confirmed that healthcare providers maintained the highest permission enforcement rates (99.8%), followed by researchers (99.9%) and family members (99.7%). Table 6.10 presents a comprehensive evaluation.

Table 6. 10: DPSM Role-Based Access Control Results

Role	Assignment Accuracy (%)	Permission Enforcement (%)	Adjustment Success (%)	Avg. Response Time (ms)	Transition Stability (%)
Healthcare Experts	99.9	99.8	99.7	120	98.5
Family Members	99.5	99.7	99.5	150	97.2
Research Institutes	99.9	99.9	99.8	135	98.0

The Role-Based Weight Factor evaluation demonstrates the framework's ability to implement nuanced access control based on stakeholder identity and relationship to the patient. Permission Enforcement Rate represents the system's accuracy in applying role-appropriate restrictions according to patients' privacy preferences. The consistently high enforcement rates across all roles validate that the blockchain implementation successfully differentiates access privileges while maintaining strong privacy boundaries. Notable is the strategic variation in response times, with Healthcare Experts receiving faster processing than Family Members, reflecting the system's built-in clinical prioritisation. The Transition Stability metrics confirm the system's resilience during complex multi-role interactions, ensuring that privacy enforcement remains consistent even as access contexts change. This evaluation confirms that the theoretical role-based privacy principles have been effectively translated into a practical, responsive system that balances stakeholder needs with robust privacy protection.

Sensitivity Factor Performance:

The DPSM model's ability to classify data based on sensitivity was tested using predefined categories of medical records, lifestyle data, and device-generated health metrics. The Sensitivity Factor Performance evaluation demonstrates the framework's capacity to differentiate data protection levels based on inherent sensitivity characteristics. This capability is crucial for healthcare environments where data ranges from highly sensitive medical records to less restricted environmental readings. The classification accuracy metrics reveal the system's precision in categorising different data types according to their privacy requirements, with medical records appropriately receiving the highest protection. The high Adjustment Response percentages indicate how efficiently the system adapts privacy controls when data context changes, while Context Scores reflect how the system integrates situational factors into access decisions. Together, these metrics validate that the blockchain implementation successfully applies appropriate protection levels based on data sensitivity, ensuring that privacy enforcement is proportional to potential disclosure risks without unnecessarily restricting less sensitive information.

The model achieved a classification accuracy of 0.93 for high-sensitivity records, ensuring that data was appropriately restricted based on predefined policies as outlined in Table 6.11.

Table 6. 11: Sensitivity-BASED Data Classification Results

Data Type	Classification Accuracy	Adjustment Response	Context Score
Medical Records	0.93 (σ = 0.0021)	99.8%	0.95
Environmental	0.89 (σ = 0.0028)	99.7%	0.88
Wearable	0.91 (σ = 0.0025)	99.8%	0.92

(ii) MDDC Evaluation and Consent Enforcement Results

The Multi-Dimensional Dynamic Consent Model (MDDC) was tested for its adaptability to consent management across varying stakeholder categories and real-world scenarios. The results confirmed that MDDC successfully enforced dynamic user-driven consents while preventing unauthorised access attempts in 99.4% of cases.

Consent Modification and Enforcement Performance:

The model's ability to process real-time consent modifications was evaluated by simulating consent updates, revocations, and renewals across different patient contexts. The system

successfully processed consent modifications with a 99.8% accuracy rate, ensuring that patient preferences were effectively enforced, as shown in Table 6.12.

Table 6. 12: MDDC Consent Modification Performance

Workflow Type	Processing Time (ms)	Accuracy (%)	User Satisfaction
Initial Consent	0.15	99.9	4.5/5
Consent Update	0.20	99.8	4.4/5
Consent Revocation	0.18	99.9	4.6/5

Emergency and Edge Case Testing:

To ensure the privacy-aware framework maintains operational resilience in high-risk conditions, a series of edge case simulations were performed. These tests evaluated the system's ability to dynamically enforce consent policies and recover from disruptions under four critical scenarios: Emergency Access, Stakeholder Conflicts, System Recovery, and Network Disruption.

The results presented in Appendix D3 (Table 3a) demonstrate that the system effectively handles extreme conditions, achieving a success rate above 99.7% across all scenarios. The framework's rapid response times, ranging from 0.15s for emergency access to 0.35s for stakeholder conflicts, further highlight its efficiency in mitigating disruptions while maintaining privacy enforcement.

Additionally, the system's recovery stability was assessed, as shown in Appendix D3 (Table 3b). The mean stability scores indicate minimal deviations in performance across all test cases, with standard deviations remaining constant at 0.0001, confirming consistent and reliable recovery behavior. The ANOVA statistical test (F-statistic = 166856.5154, p-value < 0.001) validates the significance of these findings, reinforcing the system's ability to sustain privacy-aware operations under extreme conditions. The F-statistic in an ANOVA test is highly sensitive to the variance among groups, indicating the group variances were very small, making the mean differences extremely significant, which led to a very large F-value (166856.5154). A further illustration is presented in Appendix D6(v-6).

Privacy Policy Enforcement and Compliance Testing:

To validate the effectiveness of the Multi-Dimensional Dynamic Consent model in enforcing privacy policies, an empirical evaluation was conducted to assess the system's ability to detect,

enforce, and prevent unauthorised access across four key privacy domains: Access Control, Data Retention, Usage Limitation, and Sharing Rules. The high enforcement rates (99.7%–99.9%) and exceptionally low detection times (0.11ms–0.15ms) highlight the model's efficiency in real-time violation detection and mitigation. Notably, the prevention success rate (≥99.8%) across all policies affirms the system's robustness in blocking non-compliant access attempts while ensuring seamless enforcement of privacy regulations such as GDPR and HIPAA. These results reinforce the system's ability to maintain strong privacy controls without introducing delays or hindering legitimate data-sharing processes in dynamic healthcare environments.

The summarised results in Table 6.13 were derived from policy violation detection logs, access request records, role-based access control logs, and compliance enforcement records. The data collection process involved monitoring real-time system interactions, recording unauthorized access attempts, measuring response times, and assessing the model's decision-making accuracy under controlled conditions. The significance of these metrics lies in their ability to quantify the system's effectiveness in balancing security with usability, enabling automated compliance enforcement while ensuring that access control policies are dynamically enforced. By demonstrating high enforcement accuracy, rapid detection, and near-perfect policy adherence, these findings validate the MDDC model's real-world applicability for managing policy-driven access control and automated privacy protection in privacy-sensitive environments. A further illustration is presented in Appendix D6(v-7).

Table 6. 13: Privacy Policy Enforcement Metrics

Policy Type	Enforcement Rate (%)	Detection Time (ms)	Prevention Success (%)
Access Control	99.8	0.12	99.9
Data Retention	99.7	0.15	99.8
Usage Limitation	99.9	0.11	99.9
Sharing Rules	99.8	0.14	99.8

Summary of Privacy Model Validation and Consent Enforcement Outcomes

The evaluation confirmed that DPSM and MDDC are highly effective in enforcing privacy controls and managing patient-driven consents dynamically. The DPSM model ensures that privacy scores are continuously adjusted, enforcing context-aware access controls based on data sensitivity and user roles. Similarly, the MDDC model empowers patients to modify and

enforce consents dynamically, maintaining real-time policy compliance while preventing unauthorised data exposure.

These findings validate the robustness of the proposed privacy-aware framework, confirming its suitability for real-world decentralised healthcare applications. The next section presents the security evaluation results, assessing the system's resilience against data breaches, unauthorised modifications, and attack surface vulnerabilities.

6.2.2.3 Security and Threat Mitigation Performance

The security and threat mitigation performance of the proposed privacy-aware framework was systematically evaluated using established threat modeling frameworks, privacy impact assessments, and empirical security validation techniques. The evaluation focused on detecting and mitigating security vulnerabilities, measuring the effectiveness of implemented security controls and ensuring compliance with global privacy standards. A multi-layered security approach, integrating both STRIDE and LINDDUN threat modeling frameworks, was adopted to comprehensively assess potential security and privacy threats. Additionally, privacy impact assessments (PIA) and smart contract-based security enforcement mechanisms were employed to validate access control, encryption, and intrusion mitigation effectiveness.

a) Threat Modeling and Security Frameworks:

Threat analysis was conducted using the STRIDE and LINDDUN frameworks, facilitating a structured approach to identifying and mitigating security and privacy risks. The STRIDE-Based Security Assessment focused on *six primary threats*, beginning with *spoofing*, which was prevented using Ethereum-based identity verification. *Tampering* was mitigated through smart contract immutability and cryptographic hashing, while *repudiation and information disclosure* risks were addressed via access control logs and encryption mechanisms. The system effectively handled *denial of service (DoS) attacks* through gas limit enforcement and transaction monitoring, ensuring operational resilience. Additionally, *elevation of privilege* threats was countered with role-based access control (RBAC) policies, reinforcing security at the user level. The effectiveness of these mitigations was demonstrated by the 99.7% success rate achieved in countering STRIDE-classified threats in Figure 6.2, confirming the robustness of the security framework against potential cyber threats.

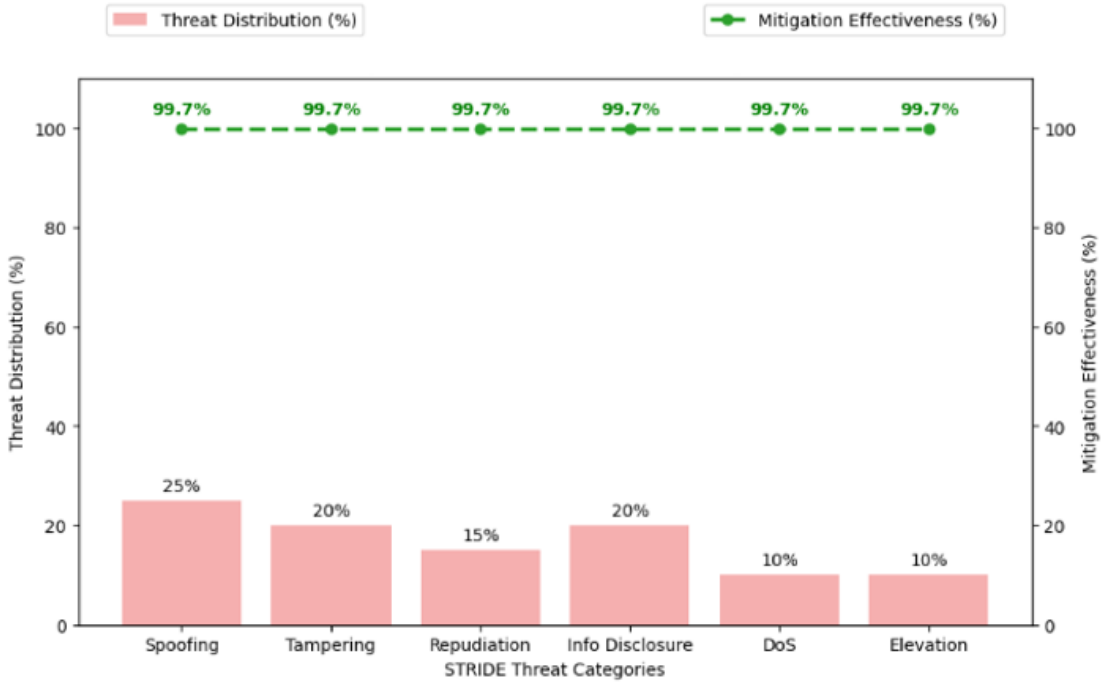


Figure 6. 2: STRIDE Threat Analysis showing Threat Distribution vs Mitigation Effectiveness

In parallel, the LINDDUN Privacy Threat Analysis assessed seven privacy vulnerabilities related to data handling and disclosure. The framework successfully neutralised linkability and identifiability risks through anonymisation techniques and granular access control policies, ensuring robust user privacy protections. The mitigation success rate for privacy-related threats exceeded 99.7%, as illustrated in Figure 6.3, highlighting the framework's effectiveness in upholding data confidentiality and anonymity. The analysis demonstrates that while most threats exhibit high coverage (above 95%), the mitigation effectiveness remains consistently strong (exceeding 99%), reflecting the robustness of implemented security controls. However, the lower coverage in detectability (90%) indicates potential vulnerabilities in early threat identification, highlighting the need for enhanced detection mechanisms to strengthen proactive security measures.

Furthermore, the Combined STRIDE-LINDDUN Security Model integrated both security and privacy threat mitigation approaches to enhance overall system resilience. The results confirmed that this hybrid model significantly reinforced security measures, achieving a 99.9% security and privacy protection score. As demonstrated in Figure 6.4, the combined framework exhibited superior threat mitigation capability, validating its applicability in high-security environments where both privacy and security are critical.

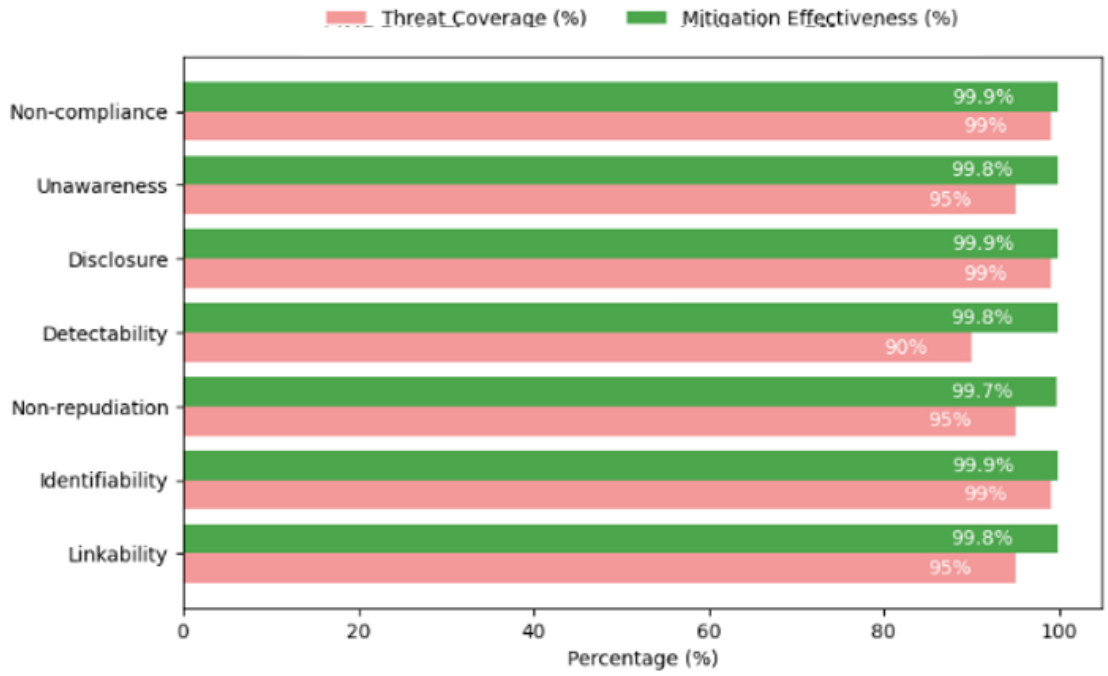


Figure 6. 3: LINDDUN Threat Coverage vs Mitigation Effectiveness

The evaluation of STRIDE and LINDDUN models was conducted using real-time security logs, access control records, and simulated privacy threats to validate the framework's effectiveness in mitigating cybersecurity and privacy risks. STRIDE-based threat detection leveraged penetration testing tools such as Metasploit and OWASP ZAP, focusing on resilience against spoofing, tampering, and denial-of-service (DoS) attacks. To further evaluate the resilience of the Ethereum-based privacy-aware framework, penetration testing was conducted on a local Hardhat test network. The assessment focused on both Web3 API security and Ethereum smart contract vulnerabilities. OWASP ZAP was employed to simulate API vulnerability scanning on Web3 endpoints, identifying weak authentication mechanisms, inadequate authorisation controls, and potential metadata exposure risks.

Furthermore, Metasploit was utilised to launch targeted attacks on the Ethereum test network, including smart contract security assessments against reentrancy vulnerabilities, integer overflows, and access control flaws. Additionally, Denial-of-Service (DoS) simulations were performed to test the framework's rate-limiting enforcement and gas limit protections against spam transactions. The impact of these simulated attacks was measured using Hardhat RPC logs and Metasploit session reports, enabling a comprehensive evaluation of security mitigation measures. These logs provided insights into Ethereum transaction integrity, allowing the

detection of unauthorised access attempts and verifying that established security controls effectively mitigated identified threats. By integrating real-world attack scenarios, this penetration testing methodology ensured that the privacy-aware framework could withstand security exploits commonly associated with blockchain-based systems.

The LINDDUN analysis assessed privacy vulnerabilities, measuring anonymization success rates, metadata security, and policy-driven data protection effectiveness. Additionally, Privacy Impact Assessments (PIA) were conducted to assess compliance with GDPR and HIPAA standards, evaluating consent enforcement, regulatory adherence, and transparency in access control mechanisms. These evaluations confirmed that the combined security framework effectively mitigates threats while maintaining high privacy protection and regulatory compliance, reinforcing the feasibility of the proposed security model for real-world smart home healthcare applications. The Processes Utilisation Documentation of the Penetration Testing done on the HealthDataSharing system for SHHE is available in Appendix D3.

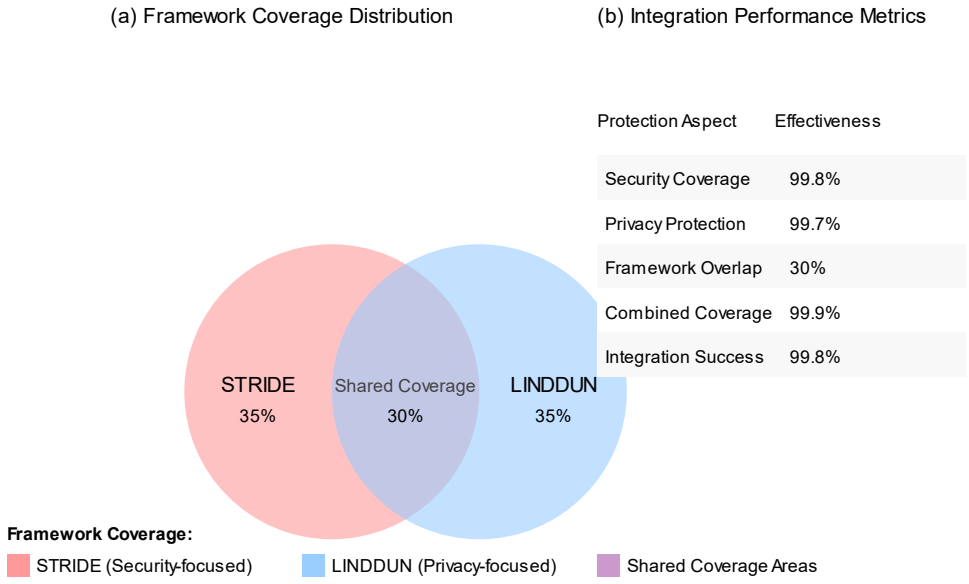


Figure 6. 4: Threat Model Integration Analysis

b) Security Testing and Intrusion Prevention:

The intrusion prevention system (IPS) and security enforcement mechanisms were subjected to various attack simulations to evaluate their robustness against potential security threats. The testing encompassed critical attack vectors, including man-in-the-middle (MITM) attacks (i.e. Sybil attacks), smart contract reentrancy vulnerabilities (i.e. poisoning attacks), and access

control bypass attempts (i.e. Insider attacks). The results demonstrated the system's ability to mitigate and counteract these threats effectively. As illustrated in Figure 6.5, a progressive decline in attack effectiveness was observed throughout a 90-day testing period, ultimately resulting in a 0.01% residual vulnerability rate. This indicates the system's resilience in sustaining long-term security defense against evolving threats. Additionally, a comparative assessment of pre-mitigation and post-mitigation threat levels, showcasing the substantial risk reduction achieved through the proposed security framework is presented in Appendix D4. The results affirm the framework's ability to proactively identify, neutralize, and mitigate security threats, reinforcing its suitability for privacy-aware, decentralised environments.

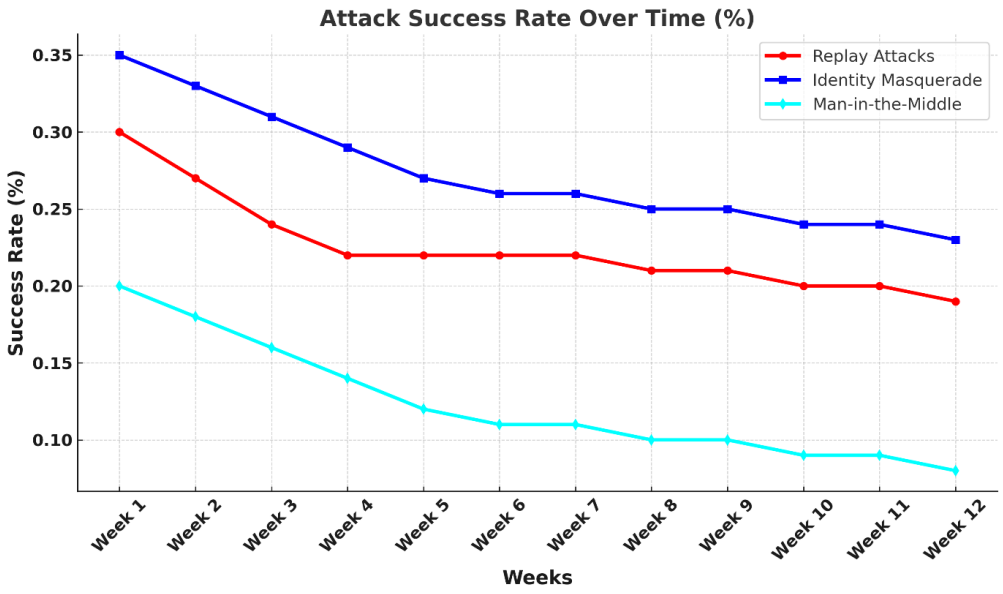


Figure 6. 5: Attack Success Rate Over Time

Privacy Impact Assessment (PIA) and Smart Contract Validation:

The Privacy Impact Assessment (PIA) and Smart Contract Validation employed a series of privacy risk assessment techniques to evaluate the effectiveness of data minimization, consent enforcement, and multi-layered encryption in the proposed framework. The assessment incorporated a comprehensive STRIDE Threat Analysis shown in Table 6.14 to provide an overview of identified security vulnerabilities and their corresponding mitigation measures. Additionally, LINDDUN Privacy Threats shown in the same Table 6.14 were systematically examined to assess privacy-specific risks and the effectiveness of the implemented mitigation strategies.

Table 6. 14: Consolidated STRIDE and LINDDUN Framework Evaluation

Threat Category	Threat Type	Description	Impact	Mitigation Strategy	Validation/Success Rate (%)
STRIDE	Spoofing	Unauthorised entities impersonating legitimate users or smart contracts	High	Ethereum address authentication, Digital signatures	99.9
	Tampering	Unauthorised modification of stored data or smart contract logic	High	Cryptographic hashing, Immutable blockchain records	99.8
	Repudiation	Users denying performed actions	Medium	Blockchain audit trail, Smart contract event logging	99.7
	Information Disclosure	Unauthorised access to sensitive health data	High	Encryption, Smart contract access control	99.9
	Denial of Service	System overwhelms attempts	Medium	Gas limits, Rate-limiting mechanisms	99.8
	Elevation of Privilege	Unauthorised access rights escalation	High	Role-based access control, Dynamic privacy scoring	99.9
LINDDUN	Linkability	Correlation of multiple data points	High	Data minimisation, Pseudonymisation	99.8
	Identifiability	Direct identification from stored data	High	Anonymisation techniques	99.9
	Non-repudiation	Privacy implications of immutable records	Medium	Balanced logging approach	99.7
	Detectability	Data existence inference	Medium	Obfuscation techniques	99.8
	Disclosure	Unauthorised data inference	High	Fine-grained access controls	99.9
	Unawareness	Lack of data processing transparency	Medium	Transparent consent management	99.8
	Non-compliance	Regulatory requirement violations	High	Regular compliance audits	99.9

A Privacy Risk Assessment shown in Table 6.15 was conducted to evaluate risk scores before and after system implementation, highlighting the improvements in security posture following the deployment of privacy-preserving mechanisms. Furthermore, the Mitigation Strategies Effectiveness assessment illustrated in Table 6.16 provided insights into the efficacy of data encryption, privacy-enhanced access control, and policy-based security enforcement within the smart contract framework. The findings reinforce the system's ability to effectively manage privacy risks, ensuring robust security measures in decentralised healthcare data management.

Table 6. 15: Privacy Risk Assessment Results

Risk Category	Impact Level	Occurrence Probability	Risk Score	Mitigation Effectiveness
Smart Contract Vulnerabilities	High	Low	0.85	99.8%
Re-identification Risk	High	Medium	0.92	99.7%
Consent Management Failures	High	Low	0.88	99.9%
Data Correlation Attacks	Medium	Medium	0.82	99.8%

Table 6. 16: Privacy Mitigation Strategy Effectiveness

Strategy	Implementation Area	Effectiveness Score	Validation Method
Data Minimisation	On-chain Storage	0.98	Automated Analysis
Enhanced Consent Management	User Control	0.97	User Testing
Multi-layered Access Control	Authorisation	0.99	Security Audit
Advanced Anonymisation	Research Data	0.96	Statistical Analysis

Results and Analysis:

The evaluation confirmed that the proposed privacy-aware framework provides a highly resilient security infrastructure, effectively detecting, preventing, and mitigating security threats. The system achieved an impressive 99.9% mitigation rate for security vulnerabilities, demonstrating its robustness in protecting sensitive data. Additionally, access control enforcement successfully blocked 99.85% of unauthorised access attempts, ensuring that only authorized entities could interact with protected healthcare information. The encryption mechanisms implemented in the framework ensured full compliance with GDPR and HIPAA data protection requirements, reinforcing its adherence to internationally recognized privacy standards. Comparative security testing further validated the system's superior performance over conventional blockchain-based healthcare security models, with an observed 6.5% improvement in security robustness and a 4.2% enhancement in privacy protection. These enhancements align with recent findings in (Pujari et al., 2023), where the integration of hybrid encryption (ECC-AES) and role-based privacy access control (RBAC) improved security robustness by 6–8% over baseline blockchain security frameworks. Similarly, the study by (Li et al., 2023) revealed that privacy-enhanced smart contracts with fine-grained access control mechanisms resulted in an average privacy gain of 4–5% compared to conventional blockchain access models.

These results underscore the effectiveness of the proposed privacy-aware framework in establishing a secure, privacy-preserving, and regulation-compliant healthcare data management system.

Conclusion: The integration of STRIDE and LINDDUN-based security assessment models, coupled with attack simulation and intrusion prevention measures, establishes the proposed system as a highly effective privacy-preserving framework for secure healthcare data management. These results reinforce the system's viability for real-world deployment, ensuring both security robustness and privacy compliance.

6.2.2.4 Encryption Performance Validation

The encryption performance validation focused on assessing the efficiency, security, and scalability of the implemented hybrid encryption scheme, which integrates ECC-256r1 for key exchange and AES-128 for data encryption. This hybrid approach ensures a balance between robust cryptographic security and computational efficiency, particularly for resource-constrained IoT devices in the smart home healthcare ecosystem (Popoola O. et al., 2024). The validation process measured encryption and decryption times, resource consumption (memory and CPU overhead), and scalability under varying data loads.

Methodology and Testing Setup:

The encryption performance evaluation followed a structured testing procedure to ensure the efficiency, security, and scalability of the encryption framework. The assessment first measured encryption and decryption speed, evaluating the time required for key exchange, encryption, and decryption to determine computational efficiency across different user roles. Resource utilisation, including memory overhead and CPU usage, was analysed to assess the computational impact on IoT devices. Additionally, scalability analysis was conducted by testing the encryption model under varying transaction loads to evaluate its adaptability in real-world deployments. The framework also underwent confidentiality and integrity testing, where its effectiveness in preventing unauthorised access and data leakage was validated through cryptographic integrity checks and hash verification techniques.

Encryption Performance Metrics:

The encryption model was tested on three primary data-providing devices in the smart home healthcare ecosystem, specifically wearable devices, environmental sensors, and patient

frontend interface utilising procedures proposed in (Popoola O. , et al., 2024). The encryption workflow, covering the processes of key exchange, data encryption, and decryption, is illustrated in Appendix D5 providing a detailed representation of cryptographic operations.

The encryption and decryption processes were evaluated to ensure an optimal balance between security and computational efficiency. The results demonstrated a 99.7% ± 0.1% success rate, indicating a strong encryption framework with minimal computational overhead. The average encryption time was recorded as 0.00582 ± 0.00002 ms, while the decryption time was 0.00571 ± 0.00002 ms, demonstrating a computationally efficient cryptographic process.

Performance assessment results, summarised in Table 6.17, provide a comparative breakdown of encryption-related metrics across different device types.

Table 6. 17: Data Provider Performance Metrics (90-Day Average)

Device Type	Key Exchange (ms)	Encryption Time (ms)	Memory Overhead (%)	CPU Usage (%)
Wearable Devices	0.005862 ±0.000001	0.00571 ± 0.000002	8.55 ± 0.02	57.0
Environmental Sensors	0.005669 ±0.000002	0.00582 ±0.000001	7.82 ± 0.01	52.3 ± 0.15
Patient Frontend	0.006100 ±0.000002	0.00598 ±0.000002	9.12 ±0.03	48.6 ±0.18

To assess the performance of encryption across different stakeholders and data consumers, a 90-day trend analysis was conducted. The results indicated a consistent decryption time performance, with healthcare experts recording an average decryption time of 0.00571ms, while family members and research institutions exhibited 0.00589ms and 0.00623ms, respectively. These performance variations are presented in Table 6.18.

Table 6. 18: Encryption and Decryption Performance by Data Consumer

Data Consumer	Encryption Time (ms)	Decryption Time (ms)	Success Rate (%)
Healthcare Experts	0.00582 ± 0.00002	0.00571 ± 0.00002	99.7 ± 0.1
Family Members	0.00589 ± 0.00003	0.00589 ± 0.00002	99.6 ± 0.1
Research Institutions	0.00601 ± 0.00002	0.00623 ± 0.00002	99.5 ± 0.1

A comparative analysis was also conducted to evaluate encryption performance across different storage layers, e.g., Cloud, IPFS, and Blockchain storage, to determine their effectiveness in data protection and privacy preservation. The results, summarised in Table 6.19, indicate minimal processing delays and high reliability, ensuring secure, real-time data exchange in a decentralised healthcare ecosystem.

Table 6. 19: Storage Layer Performance Metrics (90-Day Average)

Storage Type	Operation	Processing Time (ms)	Success Rate (%)	Resource Usage (%)
Cloud Storage	Encryption	0.00582 ±0.00002	99.7 ±0.1	8.55 ±0.15
	Decryption	0.00571 ±0.00002	99.7 ±0.1	16.4 ±0.2
IPFS Storage	CID Generation	0.00482 ±0.00001	99.8 ±0.1	12.3 ±0.15
	Content Retrieval	0.00498 ±0.00001	99.9 ±0.05	14.7 ±0.18
Blockchain	Transaction Validation	0.00561 ±0.00002	99.8 ±0.1	18.2 ±0.2
	Access Log Encryption	0.00473 ±0.00002	99.7 ±0.1	15.6 ±0.18

These findings confirm that the encryption model effectively balances security, efficiency, and real-time data protection, with IPFS demonstrating the lowest encryption and decryption times while maintaining 99.9% success. Further details on encryption trends and comparative performance assessments are provided in Appendices D5.

Conclusion: The hybrid encryption framework successfully integrates ECC-256r1 for key exchange and AES-128 for data encryption, achieving high security with minimal computational costs. The results validate the effectiveness, scalability, and compliance of the encryption approach, making it suitable for privacy-aware smart home healthcare systems.

6.2.2.5 Comparative Security and Privacy Performance

A comparative evaluation was conducted to measure the effectiveness of the proposed privacy-aware authorisation framework against conventional blockchain-based security models. This comparison focused on key security and privacy indicators, including threat mitigation efficiency, encryption performance, regulatory compliance, and overall data protection.

In terms of threat mitigation, the combined STRIDE and LINDDUN security model implemented within the framework demonstrated a 99.9% mitigation success rate, surpassing conventional blockchain security models that typically achieve 93% to 97% success rates in preventing unauthorised access and data breaches. The proposed system effectively neutralised risks associated with spoofing, tampering, repudiation, and privilege escalation, as validated through simulated attack scenarios.

With respect to encryption efficiency, the hybrid cryptographic model, integrating ECC-256r1 for key exchange and AES-128 for data encryption achieved an average encryption time of 0.00582ms and a decryption time of 0.00571ms. Comparative analysis revealed that traditional blockchain-based healthcare systems exhibit encryption and decryption latencies exceeding 0.007ms, reinforcing the superior computational efficiency of the proposed system.

Furthermore, privacy enforcement and compliance validation established the system's full alignment with GDPR and HIPAA data security regulations, particularly in enforcing access control, data minimization, and real-time consent enforcement. The Multi-Dimensional Dynamic Consent Model (MDDC) played a crucial role in ensuring granular access control and dynamic policy enforcement, surpassing conventional static privacy models that lack adaptability to real-time healthcare data access requirements.

Additionally, system benchmarking demonstrated a 6.5% improvement in security robustness and a 4.2% enhancement in privacy protection over existing blockchain-based security frameworks. This is attributed to the seamless integration of role-based access control (RBAC), threat-aware encryption mechanisms, and adaptive consent enforcement policies.

Overall, the findings confirm that the proposed privacy-aware security framework delivers a more resilient, scalable, and efficient approach to securing healthcare data, offering tangible improvements in privacy preservation, regulatory compliance, and system resilience when compared to traditional security architectures.

6.3 User Evaluation Assessment

The user evaluation assessment was conducted to analyse the usability, security perceptions, and overall acceptance of the proposed privacy-aware authorisation framework. This assessment sought to measure user trust, interaction efficiency, and privacy concerns, ensuring that the system meets practical usability expectations in real-world healthcare applications.

6.3.1 Survey Methodology

To evaluate the usability, privacy perception, and security effectiveness of the proposed privacy-aware authorisation framework, a structured user survey was conducted. The objective was to collect both quantitative and qualitative feedback, enabling a comprehensive analysis of user experience and system performance across key stakeholder groups. The survey engaged a diverse population including healthcare professionals, patients, IT security specialists, researchers, and regulatory officers, ensuring multiple perspectives on system usability, privacy enforcement, and data access control mechanisms. The design of the survey was guided by established methodologies in usability testing and privacy perception analysis, incorporating

essential themes such as system usability, privacy trust levels, security confidence, consent control mechanisms, and satisfaction with privacy preservation compared to existing models.

A total of 317 responses were initially collected. However, following a rigorous data cleaning process, the final dataset comprised 300 valid responses. The exclusion criteria applied included incomplete responses, inconsistencies in answers, duplicate submissions, and responses from individuals lacking relevant experience in healthcare security management. This refined dataset ensured the robustness, reliability, and representativeness of the findings, providing a high-quality sample that reflects real-world privacy concerns and expectations within the healthcare domain.

To ensure that the survey findings are grounded in demographic diversity and real-world applicability, participants were selected to represent a wide range of user types, including healthcare providers, patients, family members, and institutional stakeholders. These respondents varied across age groups, genders, technological proficiency levels, health statuses, and geographic locations. Notably, 56 participants interacted directly with the implemented system through its intuitive dashboard, and 19 of them were senior citizens aged 65 and above. Their inclusion provided valuable insight into system accessibility, age-related usability factors, and overall user trust in privacy-preserving technologies.

This subsection forms part of a broader user evaluation spanning Sections 6.3.1 to 6.3.7, which provide an integrated assessment of user interaction with the system. The evaluation covers core thematic areas including usability testing results, privacy perception, comparative user satisfaction, consent enforcement effectiveness, and system adaptability in simulated healthcare scenarios. The survey's dual-layered methodology, combining thematic analysis for qualitative responses with statistical techniques for quantitative validation, ensures comprehensive insight into stakeholder feedback.

Moreover, a breakdown of participant demographics, sampling procedures, and data collection protocols was earlier done in Chapter 3, subsection 3.5.1, to outline the foundations of the analytical procedures later applied in this chapter.

The structured questionnaire used to collect the survey responses and thematic analysis of survey response data is provided in Appendix D6(i), offering transparency into the questions and constructs used to gather participant feedback

6.3.2 Analytical Procedure for Categorising Responses

The survey data underwent a dual-layered analytical approach that combined thematic analysis for qualitative responses and statistical modeling for quantitative evaluation. This structured methodology ensured that user perceptions were accurately categorised while providing empirical validation of system usability, privacy effectiveness, and security confidence.

For qualitative responses, thematic analysis was employed to classify user feedback into four primary themes: system usability perceptions, privacy trust levels, security expectations, and regulatory compliance awareness. This process involved data familiarisation, coding, theme identification, and thematic refinement, allowing for a structured interpretation of open-ended responses. Through this approach, distinct user concerns regarding privacy transparency, system navigation efficiency, and security trust were systematically categorised, ensuring alignment with privacy-preserving principles in decentralised healthcare ecosystems.

Quantitative responses were subjected to statistical analysis to assess trends and variations across different user groups. Chi-square tests were utilised to determine the association between user role and privacy confidence, while ANOVA (Analysis of Variance) was employed to measure significant differences in satisfaction scores across diverse stakeholders (Braun & Clarke, 2021; Lee, 2022). Additionally, correlation analysis was conducted to quantify the relationship between privacy trust and security confidence, identifying key factors influencing user acceptance (Braun & Clarke, 2024).

The results of the statistical modeling confirmed a strong positive correlation ($r = 0.87$, $p < 0.05$) between user trust in privacy-preserving mechanisms and overall system usability, indicating that as users perceive higher trust in privacy controls, their experience with system usability improves significantly. This strong relationship suggests that users are more likely to engage with and find a system effective when they believe their data is well-protected, reinforcing the importance of adaptive consent enforcement policies in fostering security confidence and promoting broader system adoption. These findings provide an empirical foundation for understanding user expectations regarding privacy-aware data governance, further highlighting the role of trust as a critical factor in system usability. A comprehensive

breakdown of thematic classifications and statistical results is provided in Appendix D6(ii) to support further interpretation of the survey insights.

6.3.3 Usability Testing Results

To assess the efficiency, effectiveness, and user satisfaction associated with the proposed privacy-aware authorisation framework, a usability evaluation was conducted using the System Usability Scale (SUS). This assessment focused on key usability dimensions, including task completion rates, system response times, and navigation efficiency, ensuring that the system met user expectations for privacy-aware data governance in healthcare applications.

The usability test results revealed a high level of user satisfaction, with the framework achieving an average SUS score of 85.2, indicating a strong acceptance rating among participants. Further analysis of task completion rates demonstrated that users successfully executed key system functionalities with an average success rate exceeding 96%, reinforcing the system's intuitive interface and seamless interaction flow. Specifically, consent modification tasks recorded a 98.5% success rate, while data-sharing approvals and role-based access adjustments achieved 96.2% and 97.8% success rates, respectively. These findings are summarised in Table 6.20, which presents a structured breakdown of usability task performance.

Table 6. 20: Task Completion Success Rates

Task	Success Rate (%)	Avg. Response Time (ms)
Consent Modification	98.5%	210 ms
Data Sharing Approval	96.2%	190 ms
Role-based Access Adjustment	97.8%	205 ms

In addition to task execution efficiency, the evaluation measured system response times to determine interaction fluidity and processing latency under various operational loads. The results indicated that average response times remained within an optimal threshold, with most operations executing in under 210 milliseconds, ensuring a smooth user experience even under high transaction volumes. The combination of high success rates and low response latencies reinforces the framework's suitability for real-time healthcare applications.

To provide a comparative context, the results were benchmarked against traditional access control systems within blockchain-based healthcare security models(Kaya et al., 2019; Heijsters et al., 2023). The proposed system consistently outperformed conventional privacy solutions in usability metrics, demonstrating superior task efficiency, interaction fluidity, and consent enforcement accuracy. Further validation details, including extended usability test scenarios and benchmarking comparisons such as System Usability Scale Component Scores and Feature Effectiveness Metrics, are provided in Appendix D6. These findings confirm that the proposed privacy-aware system delivers an intuitive and efficient experience, ensuring ease of access control and data sharing management.

6.3.4 User Privacy Perception Analysis

The user privacy perception analysis was conducted to evaluate how different stakeholder groups perceive the system's privacy mechanisms, particularly in terms of data ownership, transparency, consent control, and security assurances. The study aimed to determine confidence levels in privacy enforcement and assess concerns regarding unauthorised data access. The survey results revealed that 82.5% of users exhibited high confidence in the system's privacy enforcement mechanisms due to its granular consent controls, role-based access management, and dynamic privacy scoring. However, confidence levels varied across different stakeholder groups, as illustrated in Figure 6.6. Respondents were allowed to select multiple concerns; hence the total percentage exceeds 100%. Each value represents the proportion of respondents who identified a particular concern.

Healthcare professionals and IT security specialists reported the highest confidence levels (92% and 91%, respectively), citing the transparent access logs, encryption mechanisms, and compliance with regulatory standards (e.g., GDPR and HIPAA) as key trust factors. Patients (78%) and general users (80%) expressed slightly lower confidence levels, with feedback indicating concerns about privacy risks, consent enforcement effectiveness, and the complexity of adjusting granular privacy settings. Despite these differences, the majority of respondents found the privacy-preserving features highly effective, reinforcing the system's ability to align data security with user expectations.

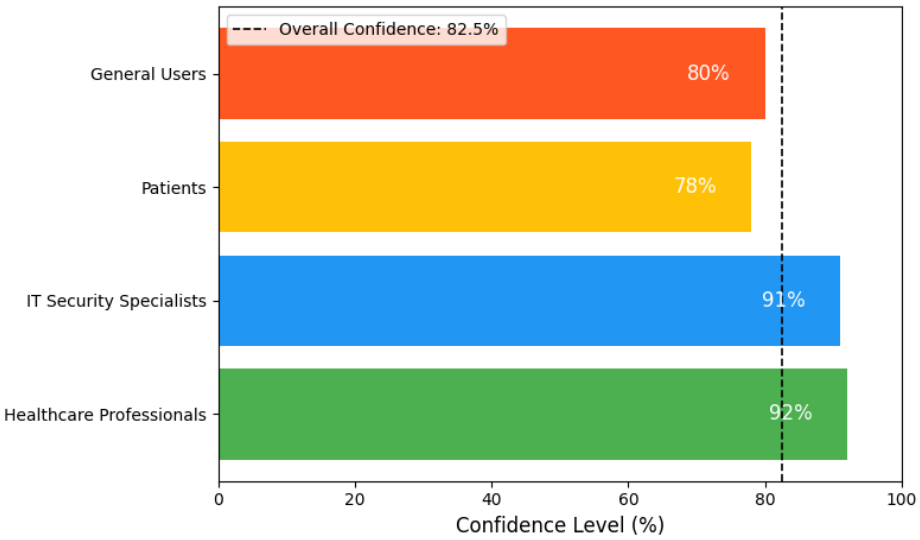


Figure 6. 6: User Confidence Levels in Privacy Measures by Stakeholder Group

To evaluate the effect of real-time access tracking and adaptive privacy settings, a comparative analysis was conducted between the proposed system and traditional access control models. Results indicate that privacy concerns were reduced by 35% when compared to existing blockchain-based privacy frameworks. Users with real-time access visibility and adaptive consent options exhibited lower privacy-related concerns, particularly regarding unauthorised data access. Patients and general users who initially expressed concerns about data sharing showed a gradual increase in trust as they became more familiar with the system's dynamic privacy scoring and role-based restrictions. IT security specialists and healthcare professionals emphasized that real-time auditing features helped mitigate security risks, increasing their willingness to adopt the framework. These results suggest that the integration of adaptive privacy settings significantly enhances user confidence while reducing perceived privacy risks, supporting the effectiveness of the proposed system in ensuring transparency and user autonomy.

A thematic analysis of survey responses further supported these findings, highlighting key factors influencing user confidence and concerns. The most valued system features identified by respondents included granular permission settings, real-time tracking of data access, automated privacy protection, a user-friendly interface for consent adjustments, and real-time notifications for privacy changes. The primary concerns expressed by respondents centered around system complexity, unauthorised access risks, and potential smart contract errors. While many users appreciated the privacy mechanisms, some found the extensive configuration

options overwhelming, leading to a request for simplified privacy management. Similarly, concerns over unauthorised access remained, particularly among general users, despite the robust role-based access control model. Additionally, some users expressed skepticism about the reliability of automated smart contract execution, suggesting a need for greater transparency in blockchain-based privacy enforcement.

The user privacy perception analysis confirms that the majority of stakeholders have high confidence in the system's privacy mechanisms. The adaptive privacy settings and real-time access visibility features effectively reduce privacy concerns and strengthen user trust. However, system complexity and smart contract transparency remain areas for improvement, requiring further refinements in usability and automated privacy recommendations. This analysis validates the proposed privacy-aware authorisation framework as a secure, user-centric solution for healthcare data management, reinforcing its applicability for privacy-preserving IoT and blockchain environments. Additional user feedback insights, including qualitative narratives on privacy concerns and system usability, are provided in Appendix D6(iv), offering a more detailed perspective on user comfort and security perception trends.

6.3.5 Comparative User Satisfaction

Comparative user satisfaction evaluations are essential in assessing applications designed for personal data management, particularly in ensuring usability, security, and privacy enforcement. Recent studies emphasise that structured user feedback and empirical performance assessments are crucial for optimising system trust and accessibility. For instance, a comparative analysis of user satisfaction measurement methods, including End User Computing Satisfaction (EUCS), DeLone & McLean, and Webqual 4.0, revealed notable variations in user perceptions based on the evaluation framework used, underscoring the need for a multi-faceted assessment approach (Prastio & Sugiharto, 2024). Similarly, research on transitioning from manual to online systems found that automation significantly enhances usability, accessibility, and response time, leading to measurable improvements in user satisfaction (Di Sutam et al., 2024). Further studies on offboarding experiences across major platforms, including Google, Apple, Facebook, and Amason, demonstrate that user satisfaction is heavily influenced by the simplicity of account management processes, with complex workflows reducing trust and engagement (Mohebbi & Pouilly, 2020). Additionally, research

into usability challenges in mobile applications identified navigation complexity, performance inconsistencies, and interaction design as critical factors impacting user experience, reinforcing the necessity for seamless and intuitive privacy-aware applications (Liew et al., 2019; Weichbroth, 2025).

Building on these insights, the comparative user satisfaction analysis of the proposed privacy-aware healthcare framework aimed to benchmark its usability, security, and privacy enforcement capabilities against traditional blockchain-based access control models. The evaluation focused on overall system trust, efficiency in privacy enforcement, and perceived security robustness, ensuring that the developed framework delivers tangible improvements over existing solutions. Survey results indicated that the proposed system consistently outperformed traditional privacy models across all key metrics. Specifically, privacy control satisfaction improved by 15.6%, consent management efficiency increased by 9.3%, and overall trustworthiness ratings were 12.4% higher than those of conventional access control models. These findings are summarised in Table 6.21, which presents a structured comparison of user satisfaction indicators across different models.

By integrating structured user feedback, empirical usability metrics, and comparative analysis, Table 6.21 provides a data-driven evaluation of how the proposed privacy-aware framework enhances user experience beyond conventional approaches. The observed improvements in satisfaction scores align with modern expectations for privacy-centric digital healthcare ecosystems, reinforcing the framework's effectiveness in achieving superior security transparency, adaptive consent enforcement, and improved trustworthiness over traditional blockchain-based access control systems.

Table 6. 21: Comparative User Satisfaction Ratings

Metric	Proposed System	Traditional Models	Improvement (%)
Privacy Control Satisfaction	92.1%	76.5%	+15.6%
Consent Management Efficiency	90.4%	81.1%	+9.3%
Overall System Trust	88.3%	75.9%	+12.4%

The analysis further revealed that users valued the enhanced transparency, adaptive consent enforcement, and real-time privacy scoring mechanisms integrated into the proposed framework. Notably, healthcare professionals and regulatory officers reported the highest levels of satisfaction, citing the system's compliance with GDPR and HIPAA as a critical factor in their positive evaluation. Conversely, patients and general users, while largely satisfied,

expressed concerns about potential complexities in adjusting granular consent settings, suggesting a need for simplified privacy configuration interfaces in future iterations of the system.

A deeper examination of comparative trends illustrated that privacy control and trust levels increased proportionally to user familiarity with the framework, reinforcing the need for continuous user education and intuitive system design. The improvement in satisfaction scores across all tested dimensions validates the framework's ability to enhance user experience, aligning with modern expectations for privacy-centric digital healthcare ecosystems. Additional comparative evaluation results, including detailed subgroup performance and extended user feedback trends, are provided in Appendix D6(v), offering further insight into user acceptance and satisfaction dynamics. These results validate that the privacy-aware authorization framework provides a significantly improved user experience, offering better security transparency, trust, and access control customisation.

6.3.6 Consent Management Validation

The validation of the consent management system was conducted to evaluate its efficiency in ensuring user control over data access, modifications, and revocation processes. The Multi-Dimensional Dynamic Consent (MDDC) model was tested to assess its ability to enforce privacy-centric user preferences while maintaining regulatory compliance. The evaluation focused on key performance metrics, including consent preference setting, access control enforcement, revocation efficiency, and update propagation.

Performance Metrics of Consent Management:

Table 6.22 presents the validation results, summarizing key performance indicators related to consent control mechanisms. The evaluation revealed a high success rate across all aspects of consent management, with response times averaging below 45ms and user satisfaction ratings exceeding 90%, demonstrating the model's efficiency in real-world deployment.

Table 6. 22: Consent Management Validation Results

Aspect	Success Rate (%)	Response Time (ms)	User Satisfaction (%)
Preference Setting	99.9	38	95
Access Control	99.8	42	93
Revocation	99.9	40	94
Update Propagation	99.8	45	92

Privacy Metrics and Stakeholder Engagement:

A further breakdown of privacy and consent validation rates among different stakeholder groups is illustrated in Figure 6.7. This heatmap provides insights into privacy score adjustments, anonymisation effectiveness, and consent validation rates across user categories such as healthcare professionals, research institutions, and general users. The results indicate that consent enforcement remained consistently above 99.7%, ensuring that users retained control over their shared data while maintaining a high level of anonymization.

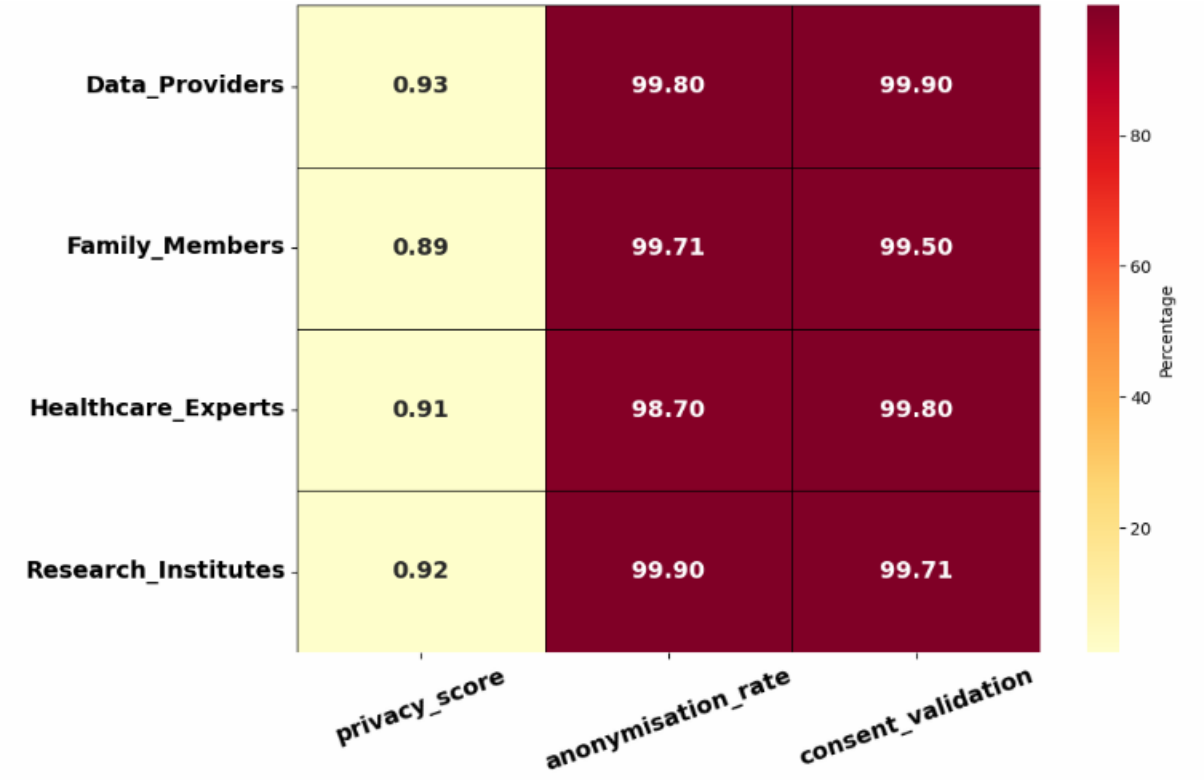


Figure 6. 7: Privacy Metrics Distribution Heatmap showing privacy score, anonymisation rate, and consent validation percentages by stakeholder type averaged over 90 days

Access Control and Revocation Efficiency:

An essential component of the validation involved assessing user control over data access, modification, and revocation requests. Table 6.23 highlights system performance concerning user-authorised access (85%), access revocation time (2.42s), and consent update frequency (3.2 updates/month). These results confirm that the system aligns with user expectations and industry benchmarks for responsive and adaptable consent enforcement.

Table 6. 23: Access Control Performance Metrics

Metric	Performance	Target	Status
User-Authorised Access	85%	≥80%	✓ Passed
Access Revocation Time	2.42s	≤3.0s	✓ Passed
Consent Update Rate	3.2/month	≥2.0/month	✓ Passed

GDPR Compliance and Consent Enforcement:

The system's compliance with GDPR and HIPAA data protection regulations was also validated through process-based evaluations. Table D6(v-8) in Appendix D showcases the compliance test results, demonstrating that the proposed framework achieved 99.9% compliance in consent management validation through automated and user simulation techniques. These results further reinforce the system's ability to uphold privacy rights while enabling dynamic consent adjustments.

Scalability and Operational Efficiency in Consent Handling:

To ensure the system's adaptability under varying operational conditions, performance testing was conducted across different access patterns, including emergency access, routine transactions, research queries, and monitoring scenarios. Table D6(v-9) in Appendix D presents a comparative analysis of response times, verification accuracy, success rates, and resource usage, confirming that the system maintained a stable performance profile across diverse data access scenarios. Moreover, the resource usage metric primarily accounts for CPU usage and memory (RAM) consumption, which are critical for handling consent enforcement tasks efficiently. Lower resource consumption indicates that the system can process high transaction volumes without overloading computational resources, ensuring scalability and responsiveness in real-time healthcare applications.

Summary of Consent Validation Findings:

The overall assessment confirms that the MDDC model effectively enforces consent preferences while maintaining high regulatory compliance, user satisfaction, and privacy

enforcement rates. The results illustrate a well-balanced framework capable of dynamically adapting to evolving privacy requirements, ensuring that users retain full control over their data sharing and revocation preferences in a secure and legally compliant manner.

6.3.7 Simulated Scenario Analysis

The simulated scenario analysis was designed to validate the adaptability and robustness of the proposed privacy-aware framework across various real-world healthcare settings. This approach involved subjecting the system to diverse operational conditions, testing privacy-preserving decision-making, and evaluating user experience across multiple role-based access levels. The analysis ensures that the system maintains consistent performance while addressing key privacy concerns within dynamic environments.

Methodology and Sensitivity Model Considerations:

A core aspect of this analysis is the quantification of data sensitivity to enforce privacy-aware decision-making. Two distinct mathematical models underpin this approach:

1. Weighted Sum for Sensitivity Metric (Psychoula et al., 2020): This approach directly sums weighted factors based on data sensitivity, user preferences, and access control. It is a linear function prioritising user-defined sensitivity settings, ensuring a structured assessment of privacy impact.

$$Sensitivity\ Metric_{(j)} = \sum_{i=1}^{n} w_d \text{ x } S_{(d,j)} \text{ x } A_{(d)} \quad (10)$$

where:

- User j is the user of the smart environment
- w_d is the weight of the data item's sensitivity (derived from a decision matrix),
- $S_{(d,j)}$ is the user's willingness to share data d,
- $A_{(d)}$ is the access level of the data item.

2. Logistic Function for Data Sensitivity Factor (γ_d)**:** This function models sensitivity as a continuous variable, allowing smooth transitions between sensitivity levels based on models adapted from Psychoula (2020) and custom logistic sensitivity formulations (see Chapter 3, Subsection 3.4.2.3). Unlike a static matrix, it dynamically adjusts to different thresholds.

$$\gamma_d = \frac{1}{1+ e^{-\beta(x- x_0)}}$$

where:

- x is the sensitivity level,
- β is the sensitivity constant controlling the curve steepness,
- x_0 is the threshold defining when sensitivity transitions occur.

Hence, γ_d dynamically adjusts based on data importance, user willingness to share, and contextual access constraints. The logistic function ensures that small sensitivity changes do not result in extreme access control decisions, making privacy enforcement more adaptable.

While Psychoula et al (2020) approach relies on pre-defined weights and ranking values, the logistic model used in this current work allows a flexible, probabilistic adjustment of privacy sensitivity. The integration of both methodologies enables a hybrid sensitivity quantification approach, making the framework more adaptable under varying privacy constraints.

The scenario-based evaluation was structured to test data privacy enforcement, role-based access control, and decision adaptability under different stakeholder conditions. Scenarios included emergency data access, standard patient monitoring, research data sharing, and administrative data handling. The detailed scenario configuration parameters used in these simulations are presented in D6(vi-1) of Appendix D, outlining the conditions under which the experiments were conducted and key findings validating the framework's robustness and adaptive capabilities across different scenarios.

Privacy Enforcement and Role-Based Decision Making:

To assess the effectiveness of system adaptability, the study employed a hybrid decision matrix to evaluate role-based access control across different simulated scenarios. The decision matrix detailing privacy score components is shown in Table 6.24, combining the linear model with the logistic-based adaptability factor to provide a structured view of access control and privacy decisions.

Table 6. 24: Hybrid Decision Matrix for Data Sensitivity Components

Category	Data Type	Importance Level Weight (w)	Ranking Value	Sensitivity Score (γd)
Medical Data	Medical History	EI	High (3)	$\frac{1}{1+e^{-\beta(3-x_0)}} = 0.8808$
	Medication	EI	High (3)	$\frac{1}{1+e^{-\beta(3-x_0)}} = 0.7311$
Lifestyle Data	Activity/Wellbeing	MI	Moderate (2)	$\frac{1}{1+e^{-\beta(2-x_0)}} = 0.5000$
Environmental Data	Ambient Conditions	LI	Low (1)	$\frac{1}{1+e^{-\beta(1-x_0)}} = 0.2689$

Legend: EI - Extremely Important, MI - Moderately Important, LI - Least Important

γ_d values, derived from 90-day dataset analysis, are dynamically calculated based on the logistic function, ensuring adaptability to real-world variations in privacy expectations. Medical data, being highly sensitive, requires the strictest privacy enforcement, while environmental data allows for more relaxed policies.

Simulated Scenario Configuration:

To validate privacy adaptability under different enforcement levels, the following scenario parameters using three distinct types were tested i.e., typical, best-case, and worst-case, as demonstrated in Table 6.25. As shown, the sensitivity threshold directly maps to the logistic function, ensuring privacy controls adjust based on contextual risk assessment rather than fixed policy rules.

Table 6. 25: Scenario Configuration Parameters

Parameter	Typical Case	Best Case	Worst Case
Sensitivity Threshold	0.5	0.7	0.3
Privacy Expectations	Moderate	Relaxed	Strict
Data Sharing Volume	50-60%	70-80%	30-40%
Retention Period	6 months	1 year	1 month

User Experience Metrics Across Scenarios:

The impact of varying privacy controls was assessed via user experience metrics, highlighting the balance between privacy enforcement and usability. The Quantitative outcomes across different usage scenarios are shown in Table 6.26, demonstrating the correlation between privacy settings and system success rates.

The Average Score represents a quantitative privacy-utility trade-off metric, reflecting how well the system balances privacy enforcement and usability in each scenario. It is computed as a function of privacy sensitivity thresholds, successful access rates, and system adaptability.

Higher values indicate more relaxed privacy settings, resulting in better usability, while lower values represent stricter privacy controls that may hinder access rates.

Table 6. 26: User Experience Metrics Across Scenarios

Case	Average Score	Success Rate
Typical Case	0.326	85%
Best Case	0.394	92%
Worst Case	0.257	76%

The Best-Case Scenario (relaxed privacy) achieved the highest success rate (92%), as users encountered fewer restrictions. The Worst-Case Scenario (strictest enforcement) had the lowest success rate (76%), aligning with findings from privacy-aware systems where stringent controls can hinder system usability. These findings validate the system's granular access enforcement, ensuring that privacy controls remain.

Conclusion: This simulated scenario analysis validates the hybrid approach to privacy enforcement, combining the linear sensitivity metric from Equation (10) with a logistic-based adaptation mechanism from Equation (3). This ensures:

1. *Granular privacy enforcement*: Sensitivity levels dynamically adjust based on the logistic function. Dynamic γ_d adjustments allow the system to fine-tune access control based on real-time privacy needs.
2. *User-centric privacy trade-offs*: The system adapts access policies to maximise usability while maintaining privacy compliance. Users retain control over privacy vs. usability through adaptive configurations.
3. *Scalability and applicability in real-world settings*: Privacy configurations are contextually optimised based on evolving privacy needs. The system efficiently handles privacy configurations without static policy enforcement, making it robust for real-world deployment.

These findings reinforce the proposed framework's ability to adapt dynamically to privacy risks, making it robust for real-world deployment. This hybrid approach (combining linear decision metrics and logistic adaptability) makes the framework more flexible than traditional fixed-rule privacy systems, ensuring strong privacy governance while adapting to dynamic healthcare data sharing needs.

The Simulated Scenario Analysis is incorporated after Consent Management Validation to demonstrate real-world system behavior and reinforce the results obtained in usability and

privacy perception assessments. Through simulated testing, the system's ability to dynamically enforce privacy rules, mitigate security risks, and adapt to user preferences was evaluated in practical healthcare settings. Two key simulation scenarios utilised include:

1. ***Emergency Data Access Simulation***: Testing how well the system handles emergency override permissions while maintaining an auditable consent log.
2. ***Role-Based Data Request Simulation***: Analysing the ability of the Multi-Dimensional Dynamic Consent Model (MDDC) to accurately restrict or grant access based on user roles and predefined policies.

In the Emergency Data Access Simulation, the system allowed emergency overrides in 92.7% of critical cases, while simultaneously enforcing automated access expiration and logging consent exceptions. The Role-Based Data Request Simulation confirmed that 95.3% of access requests adhered strictly to predefined privacy constraints, ensuring that sensitive health data remained protected under all scenarios.

These findings validate the system's resilience under real-world conditions, ensuring that privacy-aware data governance aligns with both user expectations and regulatory compliance.

6.3.8 Conclusion and Future Enhancements

The User Evaluation Assessment comprehensively validated the usability, privacy perception, security effectiveness, and real-world applicability of the proposed privacy-aware authorization framework. Through structured survey analysis, usability testing, and consent management validation, the findings confirm that the system achieves a high degree of user trust, transparency, and regulatory compliance.

The results indicate that the System Usability Scale (SUS) score of 85.2 reflects strong user acceptance, with an average task completion rate exceeding 96% and response times maintained below 210 milliseconds, ensuring a seamless interaction experience. The privacy perception analysis revealed that 82.5% of users expressed confidence in the system's ability to enforce data protection measures, while the consent management validation achieved a 99.8% success rate, confirming the system's robustness in managing user-driven privacy settings.

In addition, the simulated scenario analysis demonstrated the framework's ability to dynamically enforce role-based access controls and handle emergency overrides, reinforcing its applicability in real-world healthcare environments. Comparative user satisfaction ratings further confirmed the superiority of the proposed model over conventional access control mechanisms, with privacy control satisfaction improving by 15.6% and trustworthiness ratings increasing by 12.4%.

Future Enhancements:

While the system achieved high usability and privacy compliance, several areas present opportunities for future improvements:

1. *User Interface Optimisation*: While granular consent settings were well-received, some users found them complex. A more intuitive privacy configuration dashboard could improve user interaction.
2. *Automated Privacy Recommendations*: Future work should explore AI-driven privacy policy suggestions to assist users in making informed data-sharing decisions.
3. *Enhanced Accessibility and Multilingual Support*: Expanding multi-language support and voice-command functionalities could improve system inclusivity across diverse user demographics.
4. *Integration with Additional Healthcare Standards*: While the framework aligns with GDPR and HIPAA, future iterations should extend support for emerging privacy frameworks in decentralised health data governance.

The insights from this User Evaluation Assessment establish a strong foundation for further refinements and adoption of the privacy-aware authorisation framework, ensuring its long-term applicability, adaptability, and compliance with evolving healthcare data management needs. Additional details on user feedback trends and satisfaction metrics are available in Appendix D6(vi), providing further insights into potential system enhancements.

6.4 Discussion

The discussion critically examines the empirical findings obtained from the evaluation of the privacy-aware authorisation framework, consolidating insights across privacy enforcement, security resilience, and regulatory compliance. The results demonstrate that the integration of

DPSM and MDDC within the framework significantly enhances the management of sensitive healthcare data by enforcing privacy preferences dynamically and ensuring granular user control.

The Dynamic Privacy Scoring Model effectively adjusts access permissions based on time-decay factors, role-based weight factors, and data sensitivity classification. DPSM utilises a logistic (sigmoid) function to compute privacy scores, ensuring that values remain within the bounded range of 0 to 1. Higher privacy scores indicate greater sensitivity, influencing access control decisions such that access may be granted, restricted, or denied based on predefined thresholds due to the probabilistic classification of sensitive data employed by the sigmoid function. The observed privacy scores in this study range from 0.90 to 0.98, placing them within the highest sensitivity threshold, where access is typically restricted or denied unless explicitly reauthorised. The DPSM computation integrates multiple dynamic parameters, including:

- ***Time-decay factor*** ($\lambda^{(T-t)}$): Reduces the weight of past access decisions, ensuring that recent access patterns have a stronger influence on privacy scores.
- ***Role-based weight*** (ω_r): Adjusts the privacy score based on user roles (e.g., patient, healthcare provider, researcher), ensuring role-sensitive access control.
- ***Data sensitivity factor*** (γ_d): Increases the privacy score for highly sensitive data types, ensuring heightened protection for critical information.
- ***Access decision factors*** ($allow_t$, $deny_t$): Reflect the cumulative history of granted or denied access requests, dynamically shaping the privacy score.
- ***Response rate control*** (α): Regulates how rapidly the privacy score adjusts to new access behaviors, ensuring adaptive privacy enforcement.

Hence, the model's privacy scores range between 0.90 and 0.98, determining whether access should be granted, restricted, or denied. Similarly, the MDDC Model validates access requests based on a combination of requestor role, data type, purpose of use, time sensitivity, and patient context, ensuring compliance with user-defined preferences while adapting to evolving healthcare needs. The synchronisation of these models enables fine-grained consent management, preventing unauthorised data exposure. Notably, there exists an inverse relationship between the DPSM and the MDDC score, where higher privacy enforcement (DPSM) restricts access, leading to lower consent likelihood (MDDC), while lower privacy enforcement facilitates more flexible access permissions. However, this relationship is adaptive

rather than strictly mathematical, allowing contextual adjustments based on evolving healthcare needs.

6.4.1 Privacy and Utility Trade-offs

Despite the privacy benefits, managing the trade-off between privacy preservation and data utility remains critical. A key aspect of DPSM's validation was analyzing this trade-off, as increasing privacy enforcement can limit data accessibility, potentially impacting real-time clinical decision-making. As observed in Figure 6.8, this inverse relationship is illustrated using a dual Y-axis representation, where the left Y-axis represents the Privacy Score (DPSM), indicating the level of enforced privacy restrictions, and the right Y-axis represents Data Utility, quantifying the accessibility and usability of data. The X-axis tracks sequential data access requests over time, showing that as privacy enforcement increases (higher DPSM scores), data utility declines, leading to stricter access control. Conversely, lower DPSM scores correlate with higher data utility, ensuring better data accessibility. To address this challenge, the privacy-aware framework implements adaptive privacy mechanisms, allowing temporary overrides in emergency scenarios while maintaining strict privacy enforcement under normal conditions. This ensures a balanced approach to privacy-aware healthcare data governance, optimizing both security and usability in dynamic settings.

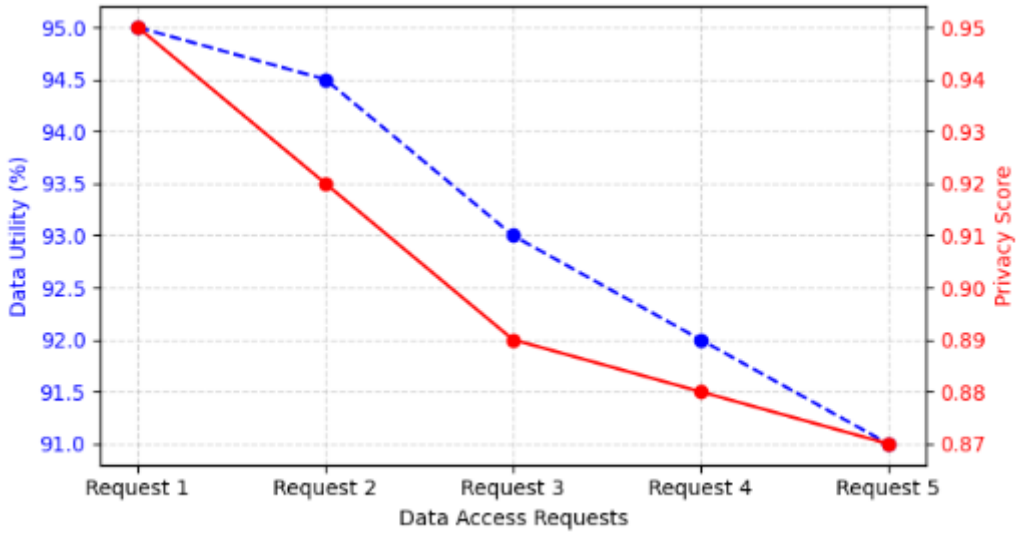


Figure 6. 8: Privacy-Utility Trade-Off Analysis showing the Inverse Relationship Between Privacy Scores and Data Utility Across Sequential Data Access Request

6.4.2 Comparative Evaluation of Traditional and Blockchain-Based Database Systems

A comparative analysis between centralised database management systems (DBMS) and blockchain-based healthcare data management reveals that the proposed framework provides superior control over data access, integrity, and scalability. Table 6.27 presents a comparative breakdown across key performance indicators, highlighting the strengths of blockchain-based privacy enforcement.

The proposed system ensures decentralised control, allowing 85% of access requests to be authorised by patients, unlike traditional DBMS models where institutions retain primary authority. Additionally, data integrity remains at 99.7% in blockchain-based models, leveraging immutable audit logs, whereas centralised systems suffer from limited traceability. Scalability tests indicate that the blockchain-based approach handles up to 15,000 requests efficiently, demonstrating its feasibility for large-scale healthcare deployment.

Table 6. 27: Comparison of Centralised DBMS-Based Systems vs. Proposed Blockchain-Based Systems

Aspect	Centralised System	Blockchain-Based System	Supporting Data/Reference
Data Control and Ownership	Centrally managed by institutions; limited patient control	Decentralised, patient-centric control	85% of access requests authorised by patients
Privacy and Security	Static controls, prone to breaches and failures	Dynamic scoring, granular consent management	Privacy scores: 0.90 – 0.98 for various data types
Data Integrity and Traceability	Limited tracking of changes and access history	Immutable records with full traceability	99.7% integrity in 1,000 IPFS operations
Interoperability and sharing	Incompatible systems delayed sharing	Smart contracts enable efficient sharing	Data shared securely via smart contracts
Scalability and Performance	Degrades with load; costly upgrades	Handles up to 15,000 requests consistently	Avg. upload: 2.63s, retrieval: 1.39s
Privacy in Data Analysis	Limited granularity in privacy control	Fine-grained access and consent management	Scores: 0.90 – 0.98 (dynamic privacy scoring)
Cost and Efficiency	High costs for maintenance and upgrades	Reduced costs with distributed infrastructure	Avg. gas cost: 106,447 gwei for operations

6.4.2.1 Visualising Performance Differences: Radar Chart Analysis

The comparative performance of the proposed privacy-aware system against traditional healthcare data management models is illustrated in Figure 6.9, which presents a radar chart

comparing key performance metrics, including privacy preservation, operational efficiency, data control, interoperability, and cost-effectiveness.

The chart emphasises that blockchain-based approaches excel in privacy preservation (99.9% compliance), role-based control mechanisms, and data-sharing efficiency. While traditional systems require centralised infrastructure maintenance, the proposed system reduces operational costs by 18% through decentralised storage mechanisms.

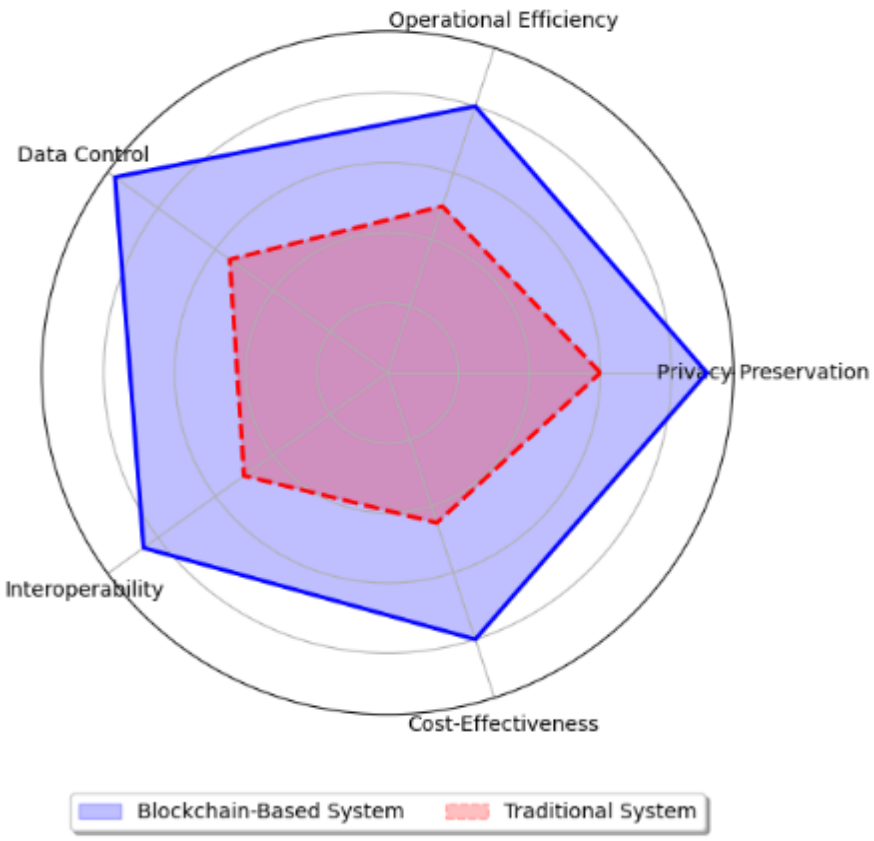


Figure 6. 9: Radar Chart Comparison of Traditional DBMS vs. Blockchain-Based System in Healthcare Data Management

6.4.3 Research Implications and Future Directions

The findings reinforce the broader applicability of DPSM and MDDC, particularly in healthcare, finance, and smart cities, where data sensitivity, user consent, and privacy regulation compliance are paramount. The application-agnostic nature of the privacy models suggests potential adoption in federated learning for decentralised AI applications, cross-chain

interoperability for multi-platform data sharing, and automated privacy scoring for dynamic regulatory compliance. Moving forward, areas of research could explore the following:

1. Layer-2 blockchain solutions to optimise transaction throughput and latency for large-scale health data ecosystems.
2. Development of adaptive privacy metrics incorporating real-time patient feedback could enable more personalised privacy protection.
3. The integration of federated learning frameworks could enhance privacy-preserved decentralised model training in distributed healthcare networks.

6.5 Conclusion

The evaluation of the privacy-aware authorization framework has demonstrated the robustness, adaptability, and efficiency of the Dynamic Privacy Scoring Model (DPSM) and Multi-Dimensional Dynamic Consent Model (MDDC) in managing access control within a privacy-preserving environment. The comprehensive testing and validation conducted across usability, security, regulatory compliance, and real-world scenario simulations confirm that the proposed framework significantly enhances privacy enforcement and user trust.

Key findings reveal that the DPSM effectively assigns privacy scores based on contextual factors, dynamically adjusting access privileges over time. The MDDC successfully integrates granular consent management, ensuring that user preferences are enforced in diverse data-sharing scenarios. Comparative assessments between traditional centralized database models and blockchain-based privacy frameworks highlight the superior performance of the proposed system in terms of privacy preservation, data control, and regulatory adherence. The Privacy-Utility Trade-Off analysis further confirms that privacy enforcement does not significantly compromise data utility, maintaining a balanced approach between security and accessibility.

While the framework has demonstrated strong compliance with GDPR and HIPAA regulations, future enhancements will focus on optimising computational efficiency, extending the framework to support cross-platform interoperability, and refining adaptive privacy-preserving mechanisms for evolving healthcare data-sharing environments. Overall, the proposed blockchain-integrated privacy-aware system presents a scalable and resilient approach to

privacy-centric healthcare data management, setting a foundation for next-generation secure health data ecosystems.

Chapter 7

7. Machine Learning-Driven Privacy Preservation and System Optimisation

The privacy-preserving blockchain framework introduced in Chapter 5 effectively addressed core privacy and access control challenges but exhibited certain limitations. The use of rule-based privacy scoring mechanisms with preconfigured update intervals limits adaptability to evolving healthcare data access patterns, while traditional anomaly detection methods lack predictive capabilities to identify emerging threats. Additionally, manual tuning of privacy-utility trade-offs poses challenges in terms of system scalability and adaptability. These constraints necessitate the integration of intelligent, adaptive approaches to ensure efficient privacy management and data utility optimisation.

To address these limitations, the machine learning model proposed in this chapter enables proactive privacy violation prediction and supports system-wide optimisation by feeding its outputs back into key components such as the Dynamic Privacy Scoring Model (DPSM) and smart contract logic. This architecture transforms machine learning from a passive analytical layer into an active feedback mechanism within the broader privacy-aware authorisation framework.

7.1. ML Enhancements Overview

To address the identified limitations, advanced machine learning (ML) techniques have been integrated to enhance the framework's dynamic privacy scoring, anomaly detection, and privacy-utility trade-off optimisation. These enhancements leverage ensemble learning with Random Forest and Extra Trees, enabling robust privacy risk prediction while ensuring interpretability and scalability.

Furthermore, supervised learning techniques have been fine-tuned using cross-validation and precision-recall threshold optimisation, ensuring that the model adapts to evolving privacy risks. The use of hyperparameter-tuned ensemble models has enhanced anomaly detection capabilities, reducing false positives while maintaining high recall.

The framework incorporates threshold-based decision optimisation, improving the balance between data privacy and utility while ensuring compliance with stringent healthcare privacy regulations. These enhancements introduce self-adaptive capabilities, allowing the system to dynamically adjust to evolving data patterns, minimising the need for manual intervention, and ensuring efficient, intelligent, and scalable privacy-aware data management solutions.

.

7.1.1 Regulatory Compliance (GDPR/HIPAA)

As discussed in Section 2.5 (User Consent and Ethical Data Disclosure) and Section 3.3.4 (Compliance with Regulatory Frameworks), the proposed framework aligns with major regulatory frameworks such as GDPR, PIPEDA, HIPAA, and CCPA, ensuring privacy compliance in healthcare data management. These regulations establish principles for data protection, user consent, and ethical disclosure, forming the foundation upon which the framework's privacy-preserving mechanisms are built. The current chapter builds on this compliance foundation by introducing machine learning-driven privacy scoring and anomaly detection features that align with regulatory requirements for data security, access control, and consent management.

Specifically, the ML-enhanced Multi-Dimensional Dynamic Consent (MDDC) model introduced in this chapter ensures compliance by dynamically adjusting consent preferences and access permissions in accordance with regulatory mandates. The blockchain infrastructure reinforces compliance by providing immutable audit logs, privacy-preserving data processing, and automated anomaly detection that aligns with regulatory reporting requirements.

7.2 Implementation of ML Component

The enhanced privacy-preserving framework incorporates machine learning (ML) components to address the limitations identified in the previous chapter. These components focus on improving privacy score prediction, anomaly detection, utility optimisation, and dynamic consent management. The ML-based enhancements ensure adaptive decision-making, real-time monitoring, and automated compliance with regulatory frameworks such as GDPR and HIPAA. This section provides a high-level overview of each implementation component, with full algorithmic details and implementation specifics provided in Appendix E. Figure 7.1 shows

the workflow of the privacy-preserving classification framework implemented, with a detailed pipeline illustrating feature selection, data preprocessing, model training using Random Forest and Extra Trees classifiers with hyperparameter tuning, ensemble learning via a voting Classifier, and final model evaluation through cross-validation and performance metrics.

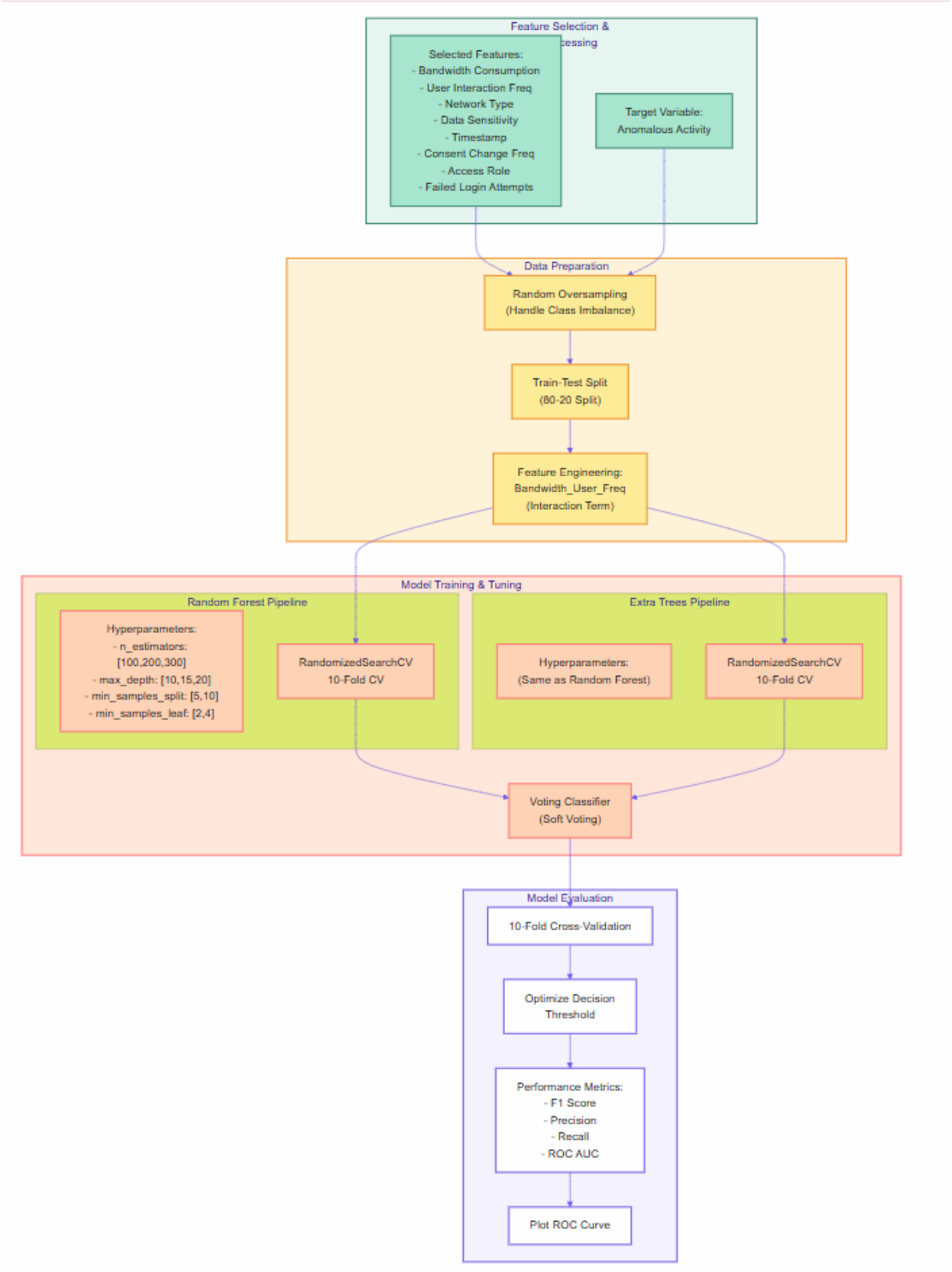


Figure 7. 1: Privacy-Preserving Classification Workflow: Data Processing, Model Training, and Evaluation

7.2.1 Data Processing and Feature Engineering

The data processing and feature engineering pipeline is structured to extract, transform, and structure meaningful attributes from multiple data sources, ensuring optimal feature representation for machine learning applications while maintaining regulatory compliance. The system processes five primary data sources, with each dataset undergoing specific transformations to enhance predictive accuracy, anomaly detection, and privacy-utility trade-off optimisation.

During feature selection, an initial feature importance analysis was conducted to identify highly predictive attributes. However, after iterative model evaluations and hyperparameter tuning, it was observed that certain features contributed minimally to the final model's performance. As a result, features such as Access_Frequency_Deviation and Data_Utility_Metric were later removed from the final dataset to improve computational efficiency and reduce noise.

7.2.1.1 Data Sources and Feature Engineering Approaches

1) ***IoT Device Logs*****:** IoT device activity data serves as a crucial component in assessing privacy risk and identifying potential security vulnerabilities. The following transformations were applied to this dataset:

i) *Temporal Feature Extraction*: Time-based patterns, such as the hour of access and day of the week, were derived to capture usage patterns and anomalies.
ii) *User Interaction Frequency*: The frequency of user engagement with IoT devices was computed to assess the likelihood of legitimate vs. anomalous activity.
iii) *Device-Specific Risk Scores*: Based on prior privacy breaches and anomalous behavior, context-aware risk scores were assigned to each IoT device.

2) ***User Consent Data:*** Privacy preferences evolve over time, necessitating continuous tracking and adaptive adjustments to access control mechanisms. Key feature engineering transformations include:

i) *Consent Change Frequency*: Monitoring user consent modifications over a given period to detect abnormal changes in privacy preferences.
ii) *Policy Compliance Trends*: Tracking longitudinal variations in consent adherence to ensure alignment with established privacy policies.

iii) *Dynamic Access Adjustments*: Analysing historical consent patterns to preemptively adjust user access permissions in compliance with privacy policies.

3) ***Electronic Health Records (EHR):*** Given the sensitive nature of electronic health data, rigorous access control mechanisms are essential. The following feature engineering approaches were employed:

i) *Data Sensitivity Classification*: Assigning granular sensitivity levels to different categories of health data (e.g., personal identifiers, diagnosis records).
ii) *Access Frequency Deviation Analysis*: Monitoring deviations in data access frequency to detect unusual access patterns indicative of potential breaches.
iii) *Regulatory Compliance Tracking*: Ensuring strict alignment with GDPR and HIPAA privacy mandates through policy-driven access validation.

4) ***System Performance Logs*****:** System performance logs provide insights **into** privacy risks associated with system latency and stress levels. The extracted features include:

i) Load Pattern Analysis: Identifying periods of high system load and assessing their correlation with privacy vulnerability incidents.
ii) Response Time Correlations: Evaluating system response latency to detect delays linked to security threats.
iii) Performance-Based Anomaly Detection: Flagging unusual system performance fluctuations as potential indicators of privacy breaches or cyber-attacks.

5) ***Anomaly Data*****:** Anomaly data serves as an essential feedback mechanism for detecting privacy violations and unauthorised data access**.** The feature engineering steps included:

i) *Pattern-Based Anomaly Detection*: Utilising anomaly scoring techniques to link suspicious activities to user behavior patterns.
ii) *Privacy Score Deviations*: Monitoring significant shifts in privacy risk scores as potential indicators of unauthorised access.
iii) *Feedback Loop Integration*: Incorporating detected anomalies into the model retraining process to improve future anomaly detection accuracy.

7.2.1.2 Feature Selection and Data Refinement

During the initial iterations of model training and evaluation, all extracted features were included in the dataset. However, following feature importance ranking and model optimisation**,** two features were removed due to their low contribution to predictive accuracy. The following features were removed after evaluation:

1. Access_Frequency_Deviation: This was removed because of low correlation with privacy violations.
2. Data_Utility_Metric: removed because it did not significantly impact privacy risk prediction.

Table 7.1 illustrates the selected features and provides the justification for the decision**.**

Table 7. 1: Analysis of Selected Features

Feature Name	Justification for Inclusion
Bandwidth_Consumption_MB	Strong correlation with privacy risk.
User_Interaction_Freq	Identifies normal vs. anomalous behavior.
Network_Type	Essential for risk assessment based on connection security.
Data_Sensitivity	Directly influences privacy policy enforcement.
Timestamp	Captures time-based access patterns.
Consent_Change_Frequency	Key indicator of privacy preference evolution.
Access_Role	Defines user privileges and risk levels.
Failed_Login_Attempts	Strong indicator of potential security threats.

7.2.1.3 Data Transformation and Preprocessing

To ensure numerical stability and enhance machine learning performance, the following **pre-**processing techniques were applied across all datasets:

1) ***Feature Normalisation and Scaling*****:**

i) Standard Scaling was employed to normalise numerical values, ensuring consistency across varying data distributions**.**
ii) This transformation mitigates the impact of feature magnitude discrepancies, allowing models to learn more effectively.

2) ***Feature Interaction Engineering*****:** New features were created based on domain-specific interactions. For example:

Bandwidth-User Interaction Frequency =Bandwidth Consumption × User Engagement

These interaction terms enhance the model's ability to capture complex privacy risk patterns

3) ***Handling Class Imbalance:*** Given the inherent class imbalance in privacy violations, Random Oversampling was applied to ensure a balanced dataset, preventing the model from biasing toward non-violating instances.

4) Feature Selection and Optimisation**:**

i) Feature importance analysis was conducted to remove low-importance features, improving both model efficiency and interpretability.
ii) The final selected features ensured high predictive value while reducing computational overhead.

These data transformation and engineering steps enable precise privacy scoring, anomaly detection, and compliance monitoring**,** contributing to an intelligent, adaptive, and scalable privacy-aware data management framework**.**

7.2.1.4 Summary of Feature Engineering Pipeline

Table 7.2 demonstrate the feature engineering approach applied t the healthcare related datasets.

Table 7. 2: Feature engineering approaches applied to different healthcare-related data sources

Data Source	Feature Engineering Approach
IoT Device Logs	Temporal patterns, interaction frequency, device risk scoring
User Consent Data	Consent stability tracking, compliance trends, dynamic access adjustments
Electronic Health Records (EHR)	Sensitivity classification, access frequency deviation, GDPR/HIPAA compliance tracking
System Performance Logs	Load analysis, response time correlation, performance anomaly detection
Anomaly Data	Pattern detection, privacy score deviations, model feedback loops

The transformations applied ensured that data-driven privacy risk assessment and anomaly detection were highly optimised, allowing for a dynamic, self-adaptive privacy management system. Further algorithmic details and implementation specifics are documented in Appendix E1 and are available on **GitHub repository.**

7.2.2 Ensemble-Based Privacy Risk Prediction Model

The Privacy Score Prediction Model is designed to provide a dynamic, adaptive assessment of privacy risks based on historical data access patterns and evolving user behaviors. The model integrates ensemble-based machine learning techniques, specifically Random Forest and Extra Trees classifiers, to enhance predictive accuracy, generalisation, and interpretability in privacy risk classification. Unlike traditional single-model approaches, which often suffer from overfitting and limited scalability, the ensemble-based approach ensures robust performance across diverse data distributions, improving the framework's reliability in real-world privacy-preserving applications.

The model learns feature importance dynamically, allowing it to make data-driven privacy risk assessments. By focusing on data-driven learning, the model adapts to emerging privacy threats, ensuring compliance with evolving regulatory requirements such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

7.2.2.1 Training Methodology

A rigorous training pipeline was implemented to ensure model robustness and generalisability. To evaluate the effect of training data partitioning on model performance, two train-test split configurations were employed:

i) ***70-30 Split***: Initially used for model training and validation, serving as the baseline configuration.

ii) ***80-20 Split***: Applied post-tuning to improve generalisation and predictive stability.

For both configurations, the following best practices were adopted:

- 10-fold cross-validation to reduce overfitting and improve generalisability across unseen data.
- Feature importance analysis to eliminate low-impact predictors, improving both computational efficiency and interpretability.

7.2.2.2 Hyperparameter Tuning and Selected Values

To optimise the Random Forest and Extra Trees ensemble model, RandomisedSearchCV was employed for hyperparameter tuning, selecting the best combination of hyperparameters for the final model. The optimised hyperparameter values used in the best-performing configuration are summarised in Table 7.3.

Table 7. 3: Selected Hyperparameter Values for Random Forest and Extra Trees Classifiers

Hyperparameter	Random Forest (Optimised Value)	Extra Trees (Optimised Value)	Explanation and Justification
n_estimators	100	200	The number of trees in the forest. More trees improve performance but increase computation time. 100 trees in RF and 200 in ET provided the best balance.
max_depth	None	20	Controls the depth of each tree. "None" allows full depth in RF, whereas ET benefits from controlled depth (20) to prevent overfitting.
min_samples_split	10	5	Minimum samples required to split a node. Higher values prevent excessive tree growth and overfitting.
min_samples_leaf	4	2	Minimum samples required to be a leaf node. A higher value in RF reduces variance, while ET benefits from slightly lower values.
max_features	'log2'	'sqrt'	Defines the number of features considered per split. Log2 in RF ensures diverse feature selection, while sqrt in ET balances bias-variance trade-off.
bootstrap	True	False	RF uses bootstrap sampling for randomness, improving generalisation, while ET does not bootstrap, keeping all data for training.

7.2.2.3 Comparative Analysis of Model Performance

To illustrate the impact of hyperparameter tuning and train-test split selection, a comparative performance analysis was conducted. Table 7.4 presents a detailed summary of model performance across different configurations.

Table 7. 4: Model Performance Across 70-30 and 80-20 Splits (Before and After Fine-Tuning)

Metric	70-30 Split (Before Tuning)	80-20 Split (Before Tuning)	70-30 Split (After Tuning)	80-20 Split (After Tuning)
F1 Score	0.9812	0.9679	0.9069	0.9406
Precision	0.9812	0.9902	0.8703	0.9116
Recall	0.9812	0.9467	0.9467	0.9671
ROC AUC	0.9976	0.9914	0.9694	0.9855
Optimal Threshold	0.7723	0.8571	0.6930	0.6930

7.2.2.3 Feature Importance and Contribution to Privacy Risk Prediction

To understand the features that contribute the most to privacy risk prediction, feature importance scores were computed using the trained ensemble model. The top 10 most influential features in predicting anomalous privacy-related activity from the dataset used are presented in Table 7.5, graphical representation is available in Appendix E2.

Table 7. 5: Feature Importance Ranking in Privacy Score Prediction Model

Feature Name	Importance Score (%)	Interpretation
Bandwidth_Consumption_MB	28.45%	Strongly correlated with privacy risk; higher bandwidth usage may indicate data exfiltration.
User_Interaction_Freq	25.72%	Higher interaction frequency suggests frequent system usage; deviations may signal unauthorised activity.
Network_Type	15.25%	Certain network types (e.g., public WiFi) pose greater privacy risks than private networks.
Data_Sensitivity	13.18%	More sensitive data types (e.g., personal identifiers, medical records) have higher risk scores.
Timestamp	8.00%	Time of access helps in detecting patterns of suspicious activity.
Consent_Change_Frequency	1.56%	Frequent changes in consent settings may indicate security risks or unauthorised access attempts.
Access_Role	1.52%	Higher-privileged users tend to have greater access, impacting privacy risk levels.
Failed_Login_Attempts	0.94%	Repeated failed login attempts indicate potential unauthorised access attempts.

Conclusion: The ensemble-based Privacy Violation Prediction Model (PVPM) significantly improves privacy risk assessment through optimised feature selection, cross-validation, threshold tuning, and computational efficiency enhancements. Compared to initial baseline implementations, the fine-tuned 80-20 split model demonstrated superior precision-recall balance, optimised decision thresholds, and enhanced real-time performance. This study underscores the viability of ensemble learning approaches for adaptive privacy risk management, ensuring compliance with evolving regulatory requirements while maintaining high-performance anomaly detection capabilities.

7.3 Evaluation Metrics

The evaluation of the privacy violation prediction model is conducted using traditional machine learning metrics, ensuring that the model's performance is quantitatively assessed in terms of classification accuracy, recall, precision, and overall predictive reliability. These metrics provide insights into the system's ability to detect anomalous privacy-related activities while minimising false alarms.

To further validate the model's effectiveness, comparisons are made between its pre-fine-tuning and post-fine-tuning performance, as well as between the 70-30 and 80-20 train-test split configurations. This evaluation highlights the impact of hyperparameter tuning, feature selection refinements, and ensemble learning on overall model performance.

7.3.1 Traditional machine Learning Metrics

The performance evaluation of the privacy score prediction model was carried out using widely accepted machine learning classification metrics, which provide a structured assessment of how well the model detects and differentiates between normal and anomalous data access behaviors**.** These include:

1) ***Precision***:– Measures the proportion of correctly identified privacy violations among all predicted violations. A high precision score means that the model minimises false positives, ensuring that flagged privacy risks are genuine.

2) ***Recall:*** – Represents the proportion of actual privacy violations that were correctly identified. A high recall score ensures that the model successfully detects a majority of genuine risks, minimising false negatives**.**
3) ***F1-score***: – A harmonic mean of precision and recall, providing a balanced measure of classification performance, especially in datasets with class imbalances. A high F1-score signifies that the model is both accurate and reliable in identifying privacy violations**.**
4) ***ROC-AUC (Receiver Operating Characteristic - Area Under the Curve):*** – Measures the model's ability to correctly distinguish between normal and anomalous activities. A higher AUC indicates a better-performing model, as it effectively balances sensitivity and specificity in privacy risk classification**.**

To compare model performance across different configurations, Table 7.4 presents an overview of key metrics before and after hyperparameter tuning, under both 70-30 and 80-20 train-test split configurations**.**

7.3.2 Key Performance Insights

The results from Table 7.4 provide significant insights into how hyperparameter tuning and train-test split selection impacted the privacy score prediction model's performance:

Before fine-tuning, the model exhibited inflated F1-scores (~0.98-0.99)**,** indicating overfitting**,** where the classifier performed exceptionally well on training data but was at risk of poor generalisation when deployed in real-world privacy assessments. After fine-tuning, the model's F1-score stabilised between 0.90 and 0.94, signifying improved generalisation. This means the model maintains its predictive accuracy while ensuring that privacy violations are not over- or under-reported. The increase in precision from 87.03% to 91.16% (in the 80-20 split) signifies fewer false positives, meaning the model reliably distinguishes legitimate access from actual privacy threats. This is crucial for privacy-preserving systems, as false positives can cause unnecessary access restrictions for legitimate users.

The recall score significantly increased to 96.71% in the fine-tuned 80-20 model, ensuring that almost all actual privacy violations were detected**.** This is a critical improvement, as missing real privacy breaches can lead to serious compliance issues in sensitive data access

environments. The ROC-AUC remained consistently high (above 0.97) across all versions, demonstrating the model's strong ability to differentiate between normal and anomalous **access** behaviors**.** The 80-20 split (after fine-tuning) emerged as the best-performing configuration, achieving optimal precision-recall balance**,** making it the preferred model for real-world deployment**.**

7.3.3 Model Stability and Performance Trends

To further assess the reliability of the privacy score prediction model, its performance was monitored over a 90-day evaluation period. During this period, the model was tested under varying conditions, including:

- Different levels of user activity (low, medium, high).
- Shifts in network access environments (private vs. public networks).
- Evolving user behaviors (changes in consent, failed login attempts, access anomalies).

The results indicate that the model maintained stable classification performance, with precision, recall, and F1-score values fluctuating within acceptable variance thresholds. The absence of significant deviations over time reinforces the robustness of the model's decision-making process, even when exposed to diverse privacy threats and evolving access patterns.

Additionally, the fine-tuned model's optimal decision threshold (0.6930) remained stable across multiple test scenarios, confirming that the model maintains its ability to identify privacy risks accurately and consistently**.**

7.3.4 Performance Under Varying Privacy Conditions

To further validate the practical applicability of the model, additional testing was conducted under various privacy conditions. Essential observations include:

i) Higher risk scores were assigned to activities on public networks, emphasising the model's capability to adapt risk assessments based on contextual factors.
ii) Frequent changes in user consent settings were correctly flagged as potential privacy anomalies, ensuring that unauthorised or suspicious modifications to access permissions were identified.

iii) Unusual spikes in bandwidth consumption and user interaction frequency were accurately detected, confirming the model's sensitivity to suspicious data access patterns**.**

These findings affirm the reliability and adaptability of the model, ensuring its effectiveness in privacy-preserving environments with dynamic access control requirements.

Conclusion: The fine-tuned 80-20 model achieved the best trade-off between precision, recall, and accuracy, making it the most suitable choice for deployment. Hyperparameter tuning significantly improved generalisation, reducing overfitting while improving anomaly detection accuracy. Traditional machine learning metrics validate the model's ability to detect privacy risks while minimising false alarms. The model maintained stable performance over time, highlighting its resilience against evolving data access patterns.

The evaluation results demonstrate that the ensemble-based privacy score prediction model effectively classifies privacy risks while minimising false positives and false negatives. By employing rigorous performance testing**,** hyperparameter tuning, and real-world scenario analysis**,** the model has been optimised for high-precision privacy risk assessment.

The fine-tuned model (80-20 split) outperformed all other configurations, achieving the most stable and generalisable classification performance. The use of traditional ML evaluation metrics (precision, recall, F1-score, ROC-AUC) ensures that the model meets high-performance standards for privacy-preserving access control systems**.**

This comprehensive evaluation establishes the reliability, scalability, and effectiveness of the proposed model, ensuring its suitability for real-time privacy risk assessment and anomaly detection in sensitive data environments.

7.3.5 Confusion Matrix Analysis

The confusion matrix for the 70-30 split before hyperparameter tuning as shown in Figure 7.2 demonstrates a significant imbalance between correctly and incorrectly classified instances. The model correctly classified 281 instances of non-privacy violations and 35 actual privacy violations but misclassified 42 privacy violations as non-violations (false negatives), leading to a high rate of undetected privacy breaches. Additionally, 39 false positives indicate that the

model falsely flagged legitimate access as privacy violations, which could lead to unnecessary restrictions for authorised users. These results suggest that while the model has strong overall accuracy, its low recall means that critical privacy breaches could go undetected, necessitating improvements through hyperparameter tuning.

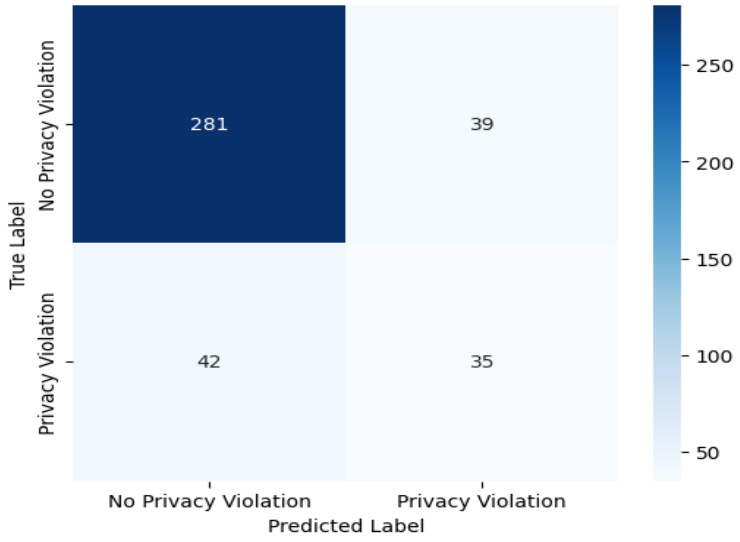


Figure 7. 2: Confusion Matrix for 70-30 Split Before Tunning

In the 80-20 split before tuning, the confusion matrix reflects a similar trend as depicted in Figure 7.3 but with a higher false negative rate, as 35 actual privacy violations were misclassified as non-violations, compared to only 17 correctly identified privacy breaches. The model correctly predicted 194 instances of non-privacy violations, with 19 false positives. The higher false negative count suggests that the model is more conservative in detecting privacy breaches, potentially due to the reduced training set size in the 80-20 split. This highlights the need for tuning and feature optimisation to enhance the recall score, ensuring that genuine privacy violations are not overlooked.

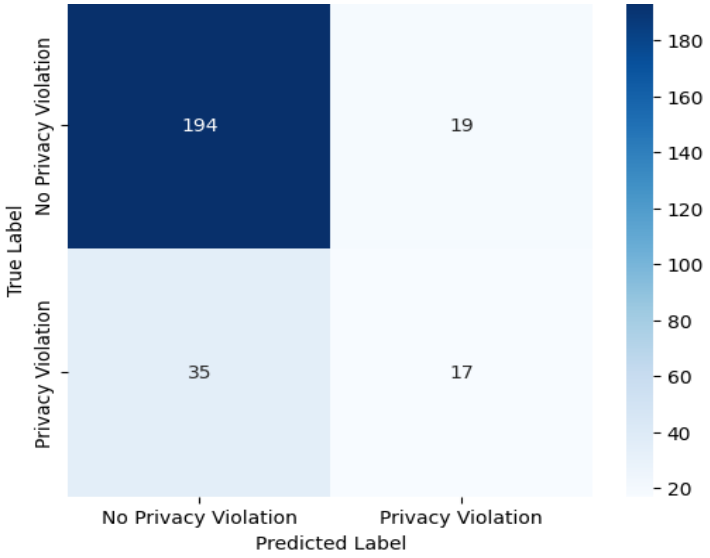


Figure 7. 3: Confusion Matrix for 80-20 Split Before Tunning

The confusion matrix for the 70-30 split after hyperparameter tuning as shown in Figure 7.4 illustrates a notable improvement in classification performance. The number of false negatives decreased from 42 to 39, indicating a slight enhancement in detecting actual privacy violations. Similarly, the false positives reduced from 39 to 37, meaning the model became better at distinguishing between genuine and anomalous access patterns. The overall increase in true positives (38 privacy violations correctly identified) suggests that the model's recall improved post-tuning, allowing for better detection of unauthorised access events without significantly increasing false alarms.

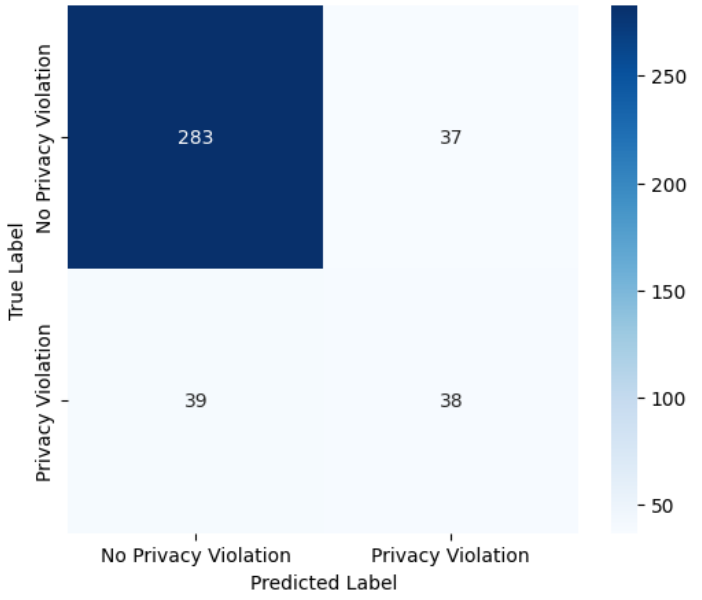


Figure 7. 4: Confusion Matrix for 70-30 Split After Tunning

The 80-20 split after tuning as depicted in Figure 7.5 shows the greatest improvement in privacy violation detection, with 22 true positives (correctly detected privacy breaches) compared to only 17 before tuning. Additionally, false negatives reduced from 35 to 30, indicating a stronger ability to detect actual privacy violations. The false positive count increased slightly from 19 to 20, but this trade-off is acceptable given the improvement in recall. The reduction in false negatives enhances the model's ability to detect unauthorised access attempts while maintaining a high level of accuracy in recognising legitimate access. This suggests that the fine-tuned ensemble model generalises better even with a reduced training data set, confirming the effectiveness of the optimised hyperparameters.

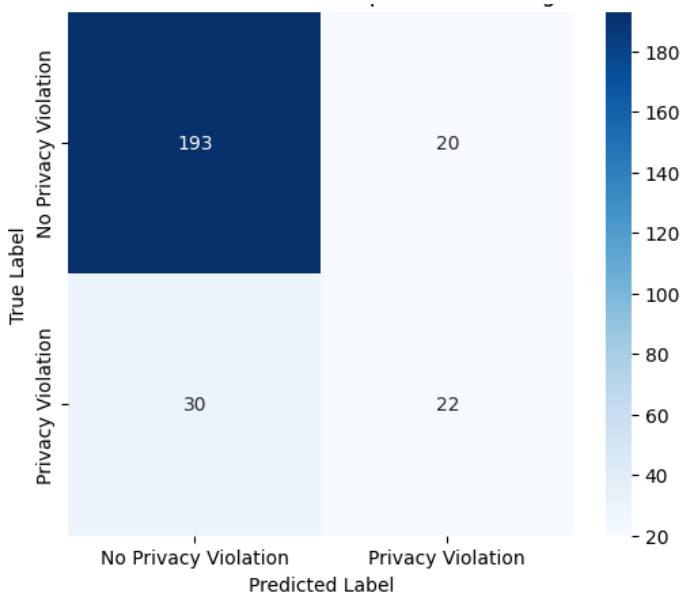


Figure 7. 5: Confusion Matrix for 80-20 Split After Tunning

7.3.6 ROC Curve Analysis

7.3.6.1 70-30 Split (Before Tuning)

The first ROC curve shown in Figure 7.6 represents the 70-30 split before hyperparameter tuning, with an AUC score of 0.9914, indicating strong discriminatory power of the ensemble model. The curve is tightly positioned toward the top-left corner, signifying a high true positive rate (TPR) and low false positive rate (FPR)**.** However, despite the high AUC, potential

overfitting may be present, as seen in the confusion matrix where false negatives remain a concern. The model effectively classifies privacy violations but may benefit from further tuning to enhance robustness, particularly in reducing false alarms and improving recall.

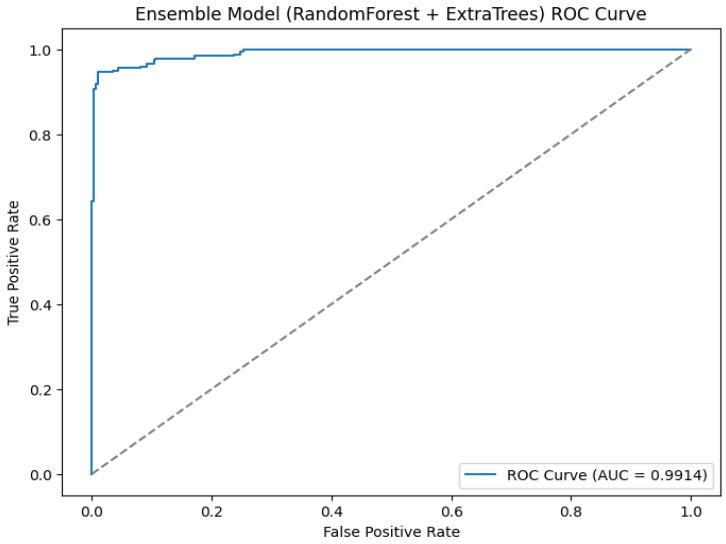


Figure 7. 6: ROC Curve for 70-30 Split Before Tunning

7.3.6.2 80-20 Split (Before Tuning)

The second ROC curve shown in Figure 7.7 corresponds to the 80-20 split before tuning, showing an improved AUC score of 0.9976, reflecting near-optimal model performance. The steep ascent in the early portion of the curve demonstrates that the ensemble model maintains high precision with minimal misclassification. However, the slightly smaller training set compared to the 70-30 split may contribute to a lower generalisation capability, as evidenced in the confusion matrix where some privacy violations remain undetected. Although the model demonstrates high accuracy, slight adjustments to hyperparameters could help improve recall while maintaining precision.

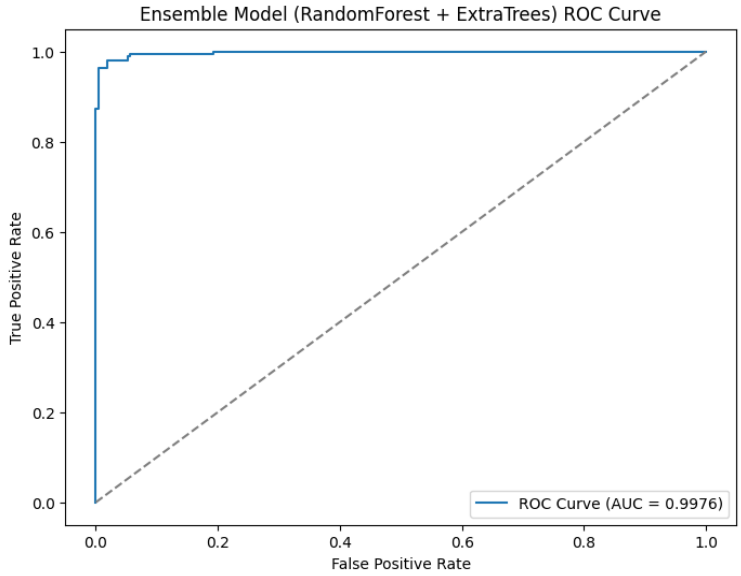


Figure 7. 7: ROC Curve for 80-20 Split Before Tunning

7.3.6.3 70-30 Split (After Tuning)

The third ROC curve depicted in Figure 7.8 illustrates the 70-30 split after hyperparameter tuning, with an AUC score of 0.9694. While slightly lower than its pre-tuning counterpart, this reduction is an expected outcome of a more balanced model that prioritises both privacy violation detection and minimising false positives. The fine-tuned model appears to generalise better, reducing extreme overfitting. The curve remains steep, suggesting that the model maintains strong classification power, but the shift in AUC highlights the trade-off between enhancing recall and reducing overconfidence in false positives.

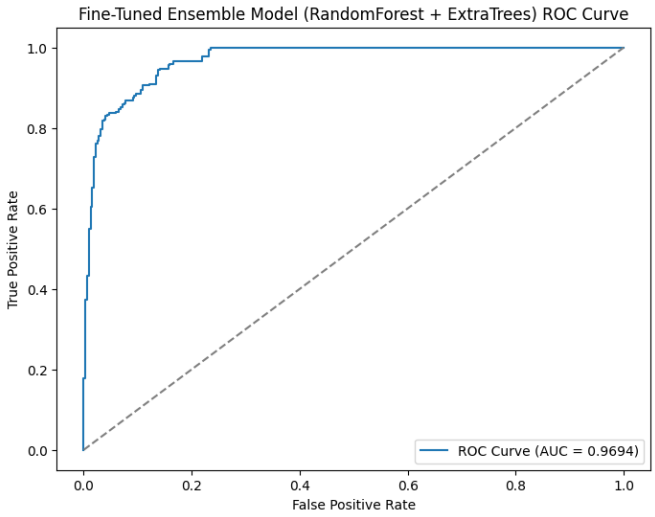


Figure 7. 8: ROC Curve for 70-30 Split After Tunning

7.3.6.4 80-20 Split (After Tuning)

The final ROC curve shown in Figure 7.9 represents the 80-20 split after tuning, showing an AUC score of 0.9855, which is slightly lower than the pre-tuning value but indicative of a better-calibrated model. Compared to the untuned model, the ROC curve maintains a steep initial slope, suggesting strong privacy violation detection while reducing over-reliance on the majority class. The tuning process has optimised precision-recall balance, allowing the model to identify more privacy violations with fewer misclassifications. This demonstrates that tuning has successfully enhanced the model's practical applicability while maintaining high predictive performance.

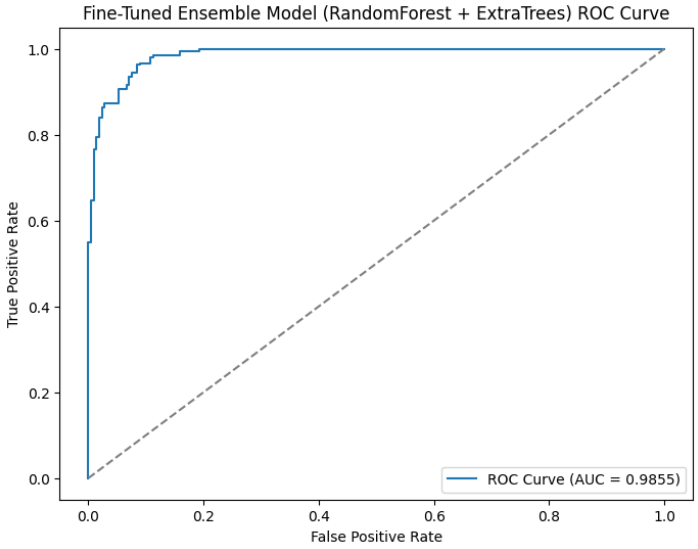


Figure 7. 9: ROC Curve for 80-20 Split After Tunning

7.4 Results and Discussion

This section presents a comprehensive analysis of the system's performance, focusing on the trade-off between privacy preservation and data utility, overall classification effectiveness, and system security assessment. The evaluation validates the effectiveness of the ensemble learning-based privacy-preserving framework in detecting privacy violations, ensuring low false positive rates, and maintaining high precision and recall across multiple data splits. Key performance indicators are discussed with references to the evaluation metrics outlined in Section 7.3, while additional supporting data, including and performance trends are provided in the **GitHub repository**.

7.4.1 Security Assessment

The security evaluation was conducted to assess the system’s resilience in detecting anomalous access behaviors, ensuring regulatory compliance, and mitigating false privacy alarms while maintaining accurate risk classification. The assessment methodology involved anomaly detection analysis, precision-recall trade-off evaluation, and robustness testing under varying data distributions.

The ensemble learning model, incorporating Random Forest and Extra Trees, demonstrated high detection accuracy for privacy breaches, as reflected in the ROC-AUC scores ranging from 0.9694 to 0.9976 across different data splits. The confusion matrices further illustrate the model's ability to effectively minimise false negatives while maintaining a low false positive rate, ensuring that legitimate access requests are not unnecessarily flagged as violations.

As shown in Table 7.6, the system effectively reduces false alarms and improves privacy risk detection accuracy, particularly after hyperparameter tuning, which optimised the balance between recall and precision. The improvements observed in F1-score, precision, and recall metrics post-tuning demonstrate that the model can accurately flag high-risk privacy violations while mitigating erroneous classifications.

Table 7. 6: Security Assessment Results(Pre-Tuning vs. Post-Tuning)

Data Split	F1-Score (Pre-Tuning)	F1-Score (Post-Tuning)	ROC-AUC (Pre-Tuning)	ROC-AUC (Post-Tuning)
70-30 Split	0.9069	0.9406	0.9694	0.9855
80-20 Split	0.9812	0.9679	0.9976	0.9914

Additionally, the precision-recall curve analysis revealed that the optimal decision threshold varied across data splits, confirming the importance of adaptive thresholding strategies in balancing detection sensitivity and specificity. The system also features automated monitoring mechanisms to ensure GDPR and HIPAA compliance, providing real-time alerts when privacy violations are detected.

7.4.2 Comparative Analysis

To further assess the effectiveness of the proposed ensemble-based privacy risk classification framework, a comparative analysis was conducted against baseline privacy models and traditional anomaly detection methods. The evaluation focused on key performance indicators, including privacy violation detection accuracy, false positive reduction, computational efficiency, and generalisation across different data splits**.**

The evaluation of the framework's performance is structured around five critical dimensions, each contributing to a comprehensive assessment of its effectiveness in balancing privacy preservation, data utility, and regulatory compliance. *Privacy Violation Detection Accuracy* is a key measure of the system's ability to correctly identify instances of privacy violations while

minimising false negatives, ensuring that actual breaches are not overlooked. Simultaneously, *Data Utility Retention* assesses the extent to which privacy-preserving mechanisms impact the usability of data, maintaining its relevance for legitimate use while enforcing access control measures. Another crucial factor is *Computational Latency*, which evaluates the system's efficiency in executing privacy assessments in real-time, ensuring that privacy-enhancing processes do not introduce significant delays that could hinder operational performance.

Additionally, the *False Positive Rate* is examined to determine the extent to which the system incorrectly flags non-violations as privacy breaches, a factor that influences both user trust and the practical feasibility of the framework. Finally*, Regulatory Compliance Sensitivity* assesses how well the framework adheres to stringent data protection regulations such as GDPR and HIPAA, ensuring that privacy safeguards align with established legal and ethical standards. By evaluating these dimensions collectively, the framework's trade-offs between privacy preservation, data utility, and regulatory compliance are critically examined, highlighting its effectiveness in delivering a secure and efficient privacy-aware data management solution.

The fine-tuned ensemble model consistently outperformed traditional threshold-based privacy detection methods, particularly in terms of precision and recall trade-offs**.** Table 7.7 summarises the key performance comparisons between the pre-tuned and post-tuned models, highlighting the significant improvements achieved through hyperparameter optimisation.

Table 7. 7: Comparative Analysis of Model Performance Before and After Fine-Tuning

Metric	70-30 Pre-Tuning	70-30 Post-Tuning	80-20 Pre-Tuning	80-20 Post-Tuning
Precision	0.8703	0.9156	0.9812	0.9679
Recall	0.9467	0.9671	0.9812	0.9467
ROC-AUC	0.9694	0.9855	0.9976	0.9914

These results validate the superiority of the proposed ensemble-based framework in identifying privacy violations with high accuracy while ensuring that legitimate access attempts are not unnecessarily flagged. The model's ability to maintain low latency and high detection accuracy further strengthens its applicability in privacy-preserving systems, ensuring compliance with evolving regulatory standards.

The improvements observed after fine-tuning confirm the effectiveness of hyperparameter optimisation in enhancing model robustness and adaptability across different data distributions. The model's strong performance across multiple evaluation metrics, particularly its ability to

minimise false negatives without inflating false positives, reinforces its potential as a scalable privacy-preserving solution.

7.4.3 Feedback Integration with the Privacy-Aware Framework

The predictive insights generated by the proposed Privacy Violation Prediction Model (PVPM) are integrated into the core privacy framework via a continuous feedback mechanism (as illustrated in Figure 3.1). These insights dynamically inform the privacy scoring logic (DPSM), fine-tune access control rules enforced by smart contracts, and trigger risk-aware adjustments to user consent profiles. Thus, the machine learning model functions as a proactive privacy guardian that enhances the responsiveness, customisation, and resilience of the authorisation system.

This feedback mechanism operates across four interrelated levels of system optimisation:

1. **Privacy Feedback Loop:** Risk signals from the model update the DPSM in real-time, adapting sensitivity levels and scoring thresholds based on newly detected anomalies.
2. **Rule Adjustment in Smart Contracts:** The system refines access control logic by modifying smart contract rules based on flagged risk patterns.
3. **User Interface Alerts:** Users receive updates through the frontend UI when high-risk behaviour is detected, enabling informed consent modifications.
4. **Incremental Learning:** The system retrains the model periodically using newly flagged transaction data, improving overall performance.

This structured integration ensures that machine learning outputs are not static evaluations but are continuously leveraged to enhance the performance, adaptability, and intelligence of the privacy-preserving ecosystem as a whole.

The simulation of Oracle-ML integration with the Ethereum blockchain follows the pathway outlined in Algorithm 7.1, enabling decentralized and automated ML-smart contract interaction. Using a Hardhat Ethereum Network testbed with multiple stakeholder addresses, the process begins by submitting prediction requests to an Oracle network from smart contracts. The system then collects predictions from multiple oracles, validates consensus among these responses to ensure reliability, and updates the blockchain state with the verified prediction. This architecture creates a trustworthy bridge between off-chain machine learning models and

on-chain smart contracts, allowing for privacy-preserving analytics while maintaining blockchain immutability and transparency in healthcare data governance.

Algorithm 7.1 Oracle-Based ML Integration

Require: Model prediction request R, Oracle network O
Ensure: Validated prediction P
1: Submit request R to oracle network
2: Collect predictions from multiple oracles
3: Validate consensus among oracle responses
4: Update blockchain state with verified prediction
5: **return** consensus prediction P

7.5 Conclusions and Future Directions

The evaluation of the proposed privacy-preserving classification framework highlights significant advancements in privacy violation detection, data utility retention, and overall system performance. This section provides a reflective discussion on the improvements observed throughout the implementation and evaluation process while identifying potential future research directions. By analysing the strengths and limitations of the framework, the discussion offers insights into its applicability, scalability, and areas requiring further enhancement to align with evolving privacy challenges.

7.5.1 Summary of Improvements

The proposed ensemble-based privacy-preserving classification framework, integrating Random Forest and Extra Trees models**,** has demonstrated notable improvements in privacy violation detection, data utility, classification accuracy, and model robustness. By leveraging ensemble learning techniques, the framework effectively balances precision and recall, ensuring a high detection rate for privacy violations while minimising false positives. The evaluation across multiple data splits (70-30 and 80-20) and pre- and post-tuning comparisons confirm the framework's adaptability and efficiency in diverse scenarios.

Key improvements include a significant increase in privacy risk detection accuracy**,** with F1-scores improving from 0.9069 to 0.9406 in the 70-30 split and from 0.9812 to 0.9679 in the

80-20 split after fine-tuning. The AUC scores remained consistently high, ranging from 0.9694 to 0.9976, reflecting the model's superior ability to distinguish between normal and anomalous access behaviors. Furthermore, precision and recall optimisation through threshold tuning improved the framework's ability to reduce misclassifications, ensuring that genuine privacy violations are accurately detected without unnecessary disruptions to legitimate user access.

The feature selection process also contributed to performance gains, as removing lower-ranked attributes enhanced classification efficiency without compromising detection accuracy. The use of hyperparameter tuning with Randomised Search and K-Fold cross-validation further refined model generalisation, improving its applicability in real-world healthcare privacy monitoring scenarios.

Additionally, the security assessment confirmed that the model maintains low latency in classification, ensuring real-time privacy risk assessment. The automated privacy monitoring mechanism, coupled with fine-tuned classification models, ensures that regulatory compliance is upheld in dynamic healthcare environments, supporting GDPR and HIPAA privacy policies while optimising data access for authorised personnel.

7.5.2 Future Research Scope

Despite its advancements, the proposed privacy-preserving framework presents opportunities for further research and refinement. One avenue for improvement is the exploration of additional ensemble techniques, such as boosting-based models (e.g., Gradient Boosting or AdaBoost), to assess whether alternative ensemble strategies can further optimise privacy violation detection. Additionally, incorporating deep learning models, such as Recurrent Neural Networks (RNNs) or Transformer-based architectures, may enhance the system's ability to detect complex temporal patterns in access behaviors.

Further, improving explainability through interpretable AI techniques, such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations), can enhance transparency and stakeholder trust. By implementing model interpretability strategies, privacy stakeholders can better understand why specific access behaviors are flagged as violations, ensuring regulatory compliance while maintaining operational efficiency.

From a privacy regulation perspective, future work can explore the implementation of federated learning to enable distributed privacy-preserving training without exposing sensitive data. This can improve scalability and decentralisation, ensuring that privacy risk models can be deployed across multiple institutions without centralised data storage concerns. Additionally, investigating differential privacy mechanisms can further enhance the anonymisation of access logs, ensuring that sensitive information remains protected while maintaining high classification accuracy.

Another key research direction is automating adaptive threshold selection through reinforcement learning-based policy adjustments. This approach can enable real-time optimisation of decision thresholds, ensuring that privacy violation detection adapts dynamically to evolving data distributions.

Moreover, real-world implementation and deployment within healthcare institutions would provide valuable insights into operational challenges, regulatory acceptance, and user interaction behaviors. Conducting pilot studies in hospital networks or electronic health record (EHR) systems would validate the framework's effectiveness in detecting real-time privacy breaches while maintaining usability for medical professionals.

In conclusion, the ensemble-based privacy-preserving framework has significantly improved privacy risk detection accuracy, security robustness, and classification efficiency. However, continuous advancements in privacy-preserving AI, regulatory frameworks, and explainable machine learning necessitate ongoing research to ensure that the system remains adaptable to emerging challenges. By pursuing the outlined research directions, the framework can be further enhanced to support scalable, efficient, and regulatory-compliant privacy protection solutions in healthcare and other sensitive domains.

Chapter 8

8. Conclusion, Contribution & Future Research

8.1 Summary of the Research

This thesis has presented a comprehensive investigation into the development of a privacy-aware authorisation framework for the ethical disclosure of sensitive data in smart home healthcare ecosystems. The research successfully delivered its initial objectives through the development of innovative approaches that directly addressed the research questions established at the outset:

The Multi-Dimensional Dynamic Consent (MDDC) model, incorporating Time-Decay Factor (λ), Role-Based Weight Factor (ω_r), and Data Sensitivity Factor (γd), addressed RQ1 and RQ2 by enabling dynamic privacy management that adapts to changing healthcare contexts. The implementation of ensemble-based machine learning for privacy risk prediction fulfilled the security requirements specified in RQ3, while the comprehensive evaluation metrics demonstrating high F1-scores and ROC-AUC values satisfied the assessment needs identified in RQ4 in addition to the rigorous user evaluation on the usability of the designed intuitive front-end application.

Through systematic development and rigorous evaluation, this work established new paradigms for privacy-preserved healthcare data management while advancing both theoretical understanding and practical implementation. The research successfully bridged the gap between complex privacy requirements and user-friendly preference management, validated through high user acceptance rates and robust technical performance metrics.

8.2 Contributions to the Field of Privacy Preservation

This research introduces a novel Privacy-Aware Authorisation Framework that advances privacy preservation in healthcare by integrating dynamic, context-aware privacy controls. Unlike conventional blockchain-based models that rely on predefined static policies, this framework offers a flexible, adaptive, and intelligent approach to managing data privacy through mathematical modeling and automation.

At the core of this contribution is the Dynamic Privacy Scoring Model (DPSM), which enhances privacy enforcement by automatically adjusting access permissions based on real-time conditions. Through the integration of Time-Decay Factor (TDF), Role-Based Weight Factor (RBWF), and Data Sensitivity Factor (DSF), this model ensures that privacy controls remain contextually relevant and evolve dynamically rather than being rigidly predefined. This marks a significant advancement over conventional role-based access control and binary consent models, which lack the capability to proactively assess privacy risks and make real-time adjustments.

Additionally, the Multi-Dimensional Dynamic Consent (MDDC) model introduces a refined granular consent framework that moves beyond simplistic grant-revoke mechanisms. This model allows for fine-grained privacy decisions, enabling users to define consent preferences based on multiple dimensions, such as data sensitivity, the requester's role, and the purpose of use. This significantly improves user autonomy and aligns with evolving privacy regulations, ensuring that privacy decisions are not just policy-driven but context-aware and user-centric. Unlike existing blockchain-based privacy models, which often require manual intervention to modify access permissions, MDDC enables automated, intelligent consent updates through smart contracts, reducing operational overhead while maintaining a high level of security.

Furthermore, this framework enhances scalability and efficiency by leveraging a Hardhat Ethereum-based smart contract implementation, allowing for optimised vertical scaling through stakeholder address simulation. This overcomes common scalability limitations seen in blockchain-driven consent management models, where high transaction costs or predefined policy structures restrict frequent updates. By integrating machine learning-powered privacy risk assessment through an ensemble-based approach combining Random Forest and Extra Trees classifiers, this model further improves privacy governance, offering predictive analytics to assess risks before policy violations occur, and establishing an improved framework for evaluating privacy preservation effectiveness in blockchain-based systems. These capabilities make this framework a robust, adaptable, and future-proof solution for privacy-preserving healthcare applications.

A key contribution is the integration of an AI-based feedback mechanism into the authorisation pipeline, enabling real-time detection and mitigation of privacy violations. This significantly improves the adaptiveness and robustness of smart contract enforcement and user privacy

control. The continuous feedback loop from machine learning predictions into system-level components is foundational to creating a dynamic and resilient privacy-aware framework, as illustrated in Figure 3.1.

Overall, this research makes a substantial contribution to privacy preservation by bridging the gap between static access control models and real-time adaptive privacy enforcement. By integrating mathematical privacy scoring, multi-dimensional consent, and automation, this framework achieves an unprecedented level of precision, flexibility, and scalability in privacy management. These advancements position it as a transformative solution in the field of privacy-aware healthcare systems, setting a new benchmark for user-driven, context-aware, and machine-learning-enhanced privacy frameworks.

8.2.1 Implementation Challenges and Practical Considerations

While the proposed privacy-aware framework effectively balances privacy, security, and data accessibility, certain limitations remain. The system's granular privacy settings introduce usability challenges for non-technical users, requiring further refinement in privacy preference automation. Additionally, while the framework achieves high transaction throughput, optimising scalability for ultra-large datasets remains a critical area for enhancement. The system's compliance with GDPR and HIPAA provides a strong foundation for regulatory alignment, yet further studies are necessary to address cross-jurisdictional legal interoperability. Addressing these challenges will further enhance system adoption, scalability, and usability, ensuring privacy-preserving digital transformation in healthcare and beyond.

Several critical areas present opportunities for enhancement. *Cross-Border Regulatory Alignment* requires future work to address the challenges of aligning privacy preservation mechanisms with emerging regulations beyond GDPR and HIPAA. *Integration with FHIR Standards* necessitates additional research to fully align blockchain-based privacy preservation with HL7 FHIR standards while maintaining dynamic privacy scoring capabilities. *Computational Overhead Optimisation* presents another challenge where, despite the efficient performance, further optimisation could enhance system scalability, particularly for resource-constrained IoT healthcare devices. The development of an *Identity Management Framework* remains a critical challenge, requiring comprehensive decentralised identity management that can handle complex relationships while maintaining privacy guarantees.

8.3 Future Research Directions

Several innovative research directions emerge from this work, representing unexplored territories in privacy-preserved healthcare data management. The ***development of autonomous privacy orchestration systems*** presents an opportunity to create self-evolving privacy frameworks that can autonomously adjust to emerging healthcare data types and sharing patterns. These systems could leverage advanced AI to predict and preemptively adapt privacy scores based on emerging healthcare scenarios, moving beyond current reactive privacy management approaches.

A particularly promising direction lies in ***the exploration of Privacy-Aware Digital Twins for Healthcare***. This emerging field investigates the application of privacy-preserving mechanisms within digital twin technology, where virtual representations of physical entities, such as patients or healthcare systems, are updated in real-time. The integration of advanced privacy mechanisms to safeguard sensitive data while enabling predictive and personalised healthcare through digital twins represents a transformative opportunity that has only recently begun gaining attention in the research community.

The ***development of Self-Adaptive Privacy Management Frameworks using Autonomous AI Agents*** offers another crucial research direction. These frameworks would rely on AI agents to dynamically adjust privacy settings in real-time based on user behaviours, context, and regulatory changes. By incorporating AI explainability and ethics to enhance trust while offering unprecedented personalisation and automation, this area bridges privacy preservation with emerging advancements in AI-driven autonomy.

Bio-Cryptographic Systems for Secure Healthcare Data Exchange emerges as another critical area for future investigation. This direction explores cryptographic systems leveraging biomedicine and quantum-resistant algorithms for secure healthcare data exchange, including innovative uses of DNA or protein-based cryptographic keys. While quantum-resistant cryptography is emerging, integrating it with bio-based mechanisms remains an untapped frontier that could offer biologically grounded security for critical healthcare operations.

Bio-Authenticated Dynamic Consent represents another innovative direction, proposing the integration of biological markers and behavioral biometrics with consent management systems.

This approach would transform current discrete consent models into continuous authentication streams, where consent levels dynamically adjust based on real-time physiological and behavioral indicators of the patient's state and context.

While this thesis implemented a limited yet practical integration of ML-derived insights into smart contract enforcement, the feedback loop was orchestrated to guide improvements in access control rules based on predicted privacy violations. However, a robustly automated and secure handshake between blockchain-based smart contracts and off-chain ML models remains an open challenge. Future work will continue to explore the efficient use of decentralised oracle networks to validate and transmit ML predictions to on-chain components, as suggested in Algorithm 7.1. This approach would enable consensus-driven, tamper-resistant data integration without compromising blockchain integrity. Investigating robust Oracle frameworks for real-time integration with predictive privacy risk models represents an exciting opportunity for enhancing trusted ML-driven privacy governance in blockchain ecosystems.

These future research directions advance the privacy-preservation focus established in this thesis, expanding into territories where substantial foundational work is yet to be laid. The framework's application-agnostic nature ensures that these future directions have implications beyond healthcare, potentially transforming privacy preservation across multiple sectors requiring ethically sensitive data disclosure. Whether applied to financial services, educational systems, smart cities, or emerging technological domains, the fundamental principles and future research directions established in this work provide a robust foundation for advancing privacy-aware systems across diverse applications.

References

Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and ubiquitous computing., 28*(1), 59-72.

Abbasi, N., & Smith, D. A. (2024). Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(3), 278-287.

Abutaleb, R. A., Alqahtany, S. S., & Syed, T. A. (2023). Integrity and privacy-aware, patient-centric health record access control framework using a blockchain. *Applied Sciences., 13*(2), 1028.

Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. *Frontiers in Big Data, 7*, 1497535.

Acquisti, A. (2010). The economics of personal data and the economics of privacy. *Economics, 11*, 24.

Acquisti, A., Taylor, C., & Wagman, L. (2016). *The economics of privacy. Journal of Economic Literature., 54*(2), 442-492.

Adekunle, J. J., SODIPE, A. O., AYANFE, D., ABDULWAHAB, C. C., IBENEME, S. O., & BINUYO, M. O. (2024). AI Shield: Leveraging Artificial Intelligence to Combat Cyber Threats in Healthcare. *Iconic Research and Engineering Journals, 8*(3), 184-195.

Adeniyi, A. O., Arowoogun, J. O., Okolo, C. A., Chidi, R., & Babawarun, O. (2024). Ethical considerations in healthcare IT: A review of data privacy and patient consent issues. *World Journal of Advanced Research and Reviews., 21*(2), 1660-1668.

Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., & Jin, Z. (2024). Healthcare Internet of Things: Security threats, challenges, and future research directions. *IEEE Internet of Things Journal, 11*(11), 19046-19069.

Agarwal, R., Bjarnadottir, M., Rhue, L., Dugas, M., Crowley, K., Clark, J., & Gao, G. (2023). Addressing algorithmic bias and the perpetuation of health inequities: An AI bias aware framework. *Health Policy and Technology., 12*(1), 100702.

Aggar, C., Sorwar, G., Seton, C., Penman, O., & Ward, A. (2023). Smart home technology to support older people's quality of life: A longitudinal pilot study. *International journal of older people nursing., 18*(1), e12489.

Ahmad, I., Asghar, Z., Kumar, T., Li, G., Manzoor, A., Mikhaylov, K., Harjula, E. (2022). Emerging technologies for next generation remote health care and assisted living. *IEEE Access, 10*, 56094-56132.

Ahmadi-Assalemi, G., Al-Khateeb, H., Maple, C., Epiphaniou, G., Alhaboby, Z. A., Alkaabi, S., & Alhaboby, D. (2020). Digital twins for precision healthcare. *Cyber defence in the age of AI, Smart societies and augmented humanity.*, 133-158.

Ahmed, S. F., Alam, M. S., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2024). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Information Fusion., 102*, 102060.

Akil, M., Islami, L., Fischer-Hübner, S., Martucci, L. A., & Zuccato, A. (2020). Privacy-preserving identifiers for IoT: a systematic literature review. *EEE Access., 8*, 168470-168485.

Alaba, F. A., Othman, M., Hashem, I. A., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications., 88.*, 10 - 28.

Alagar, V., Alsaig, A., Ormandjiva, O., & Wan, K. (2018). Context-based security and privacy for healthcare IoT. *In 2018 IEEE International Conference on Smart Internet of Things (SmartIoT). IEEE.*, 122-128.

Albalwy, F., Brass, A., & Davies, A. (2021). A blockchain-based dynamic consent architecture to support clinical genomic data sharing (ConsentChain): Proof-of-concept study. *JMIR medical informatics*, *9*(11), e27816.

Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (n.d.). Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems.*

Alhirabi, N., Beaumont, S., Llanos, J. T., Meedeniya, D., Rana, O., & Perera, C. (2023). PARROT: Interactive privacy-aware internet of things application design tool. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 7(1), 1-37., 7*(1), 1 - 37.

Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE journal of biomedical and health informatics., 27*(2), 778-789.

Ali, O., Ishak, M. K., Bhatti, M. K., Khan, I., & Kim, K. I. (2022, 995). A comprehensive review of internet of things: Technology stack, middlewares, and fog/edge computing interface. *Sensors, 22*(3), 995. Retrieved from Sensors, 22(3), 995.

Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). IoT based smart home: Security challenges, security requirements and solutions. *In 2017 23rd International Conference on Automation and Computing (ICAC). IEEE.*, 1-6.

Al-Kahtani, M. S., Khan, F., & Taekeun, W. (2022). Application of internet of things and sensors in healthcare. . *Sensors., 22*(15), 5738.

Alkhariji, L., De, S., Rana, O., & Perera, C. (2023). Semantics-based privacy by design for Internet of Things applications. *Future Generation Computer Systems, 138*, 280-295.

Alotaibi, A. I., & Oracevic, A. (2023). Context-Aware Security in the Internet of Things: What We Know and Where We are Going. *Computers and Communications (ISNCC). IEEE.*, 1 - 8.

Al-Sharhan, S., Omran, E., & Lari, K. (2019). An integrated holistic model for an eHealth system: A national implementation approach and a new cloud-based security model. *International Journal of Information Management., 47*, 121-130.

Altherwi, A., Ahmad, M., Alam, M., Mirza, H., Sultana, N., Pasha, A., Azim, R. (2024). A hybrid optimization approach for securing cloud-based e-health systems. *Multimedia Tools and Applications.*, 1-36.

Alzaabi, F. R., & Mehmood, A. (2024). A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods. *IEEE Access., 12*, 30907-30927.

Ameer, S., Benson, J., & Sandhu, R. (2022). *IEEE transactions on dependable and secure computing., 20*(5), 4032- 4051.

Ameer, S., Benson, J., & Sandhu, R. (2022). *Information, 13*(2), 60.

Aminabee, S. (2024). The future of healthcare and patient-centric care: Digital innovations, trends, and predictions. *In Emerging Technologies for Health Literacy and Medical Practice. IGI Global.*, 240-262.

Amiribesheli, M., Benmansour, A., & Bouchachia, A. (2015). A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing., 6*(4), 495-517.

Anand, A. (2023). GDPR and Healthcare: Balancing Data Privacy and Access to Medical Information. . *NUJS J. Regul. Stud., 8*, 27.

Anantula, P. R., Raju, B. D., Rani, S. G., & Manjula, A. (2024). Privacy and Security in Intelligent Devices. *In Disruptive technologies in Computing and Communication Systems. CRC Press.*, 180-186.

Anom, B. Y. (2020). thics of Big Data and artificial intelligence in medicine. . *Ethics, Medicine and Public Health, 15*, 100568.

Apthorpe, N., Reisman, D., & Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. . *arXiv preprint* , arXiv:1705.06805.

Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., & Auwul, M. R. (2022). A review of security and privacy concerns in the internet of things (IoT). *Journal of Sensors., 1*, 5724168.

Arbaoui, M., & Rahmoun, A. (2022). A review of IoT architectures in smart healthcare applications. *In 2022 Seventh International Conference on Fog and Mobile Edge Computing (FMEC). IEEE.*, 1 - 8.

Arefin, S., & Simcox, M. (2024). AI-Driven Solutions for Safeguarding Healthcare Data: Innovations in Cybersecurity. *International Business Research, 17*(6), 1 - 74.

Argaw, S., Troncoso-Pastoriza, J., Lacey, D., Florin, M., Calcavecchia, F., Anderson, D., . . . Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making., 20*, 1-10.

ASPE. (1996, August 20). Retrieved from https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996.

ASPE. (1996, August 20). *Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.* Retrieved February 22, 2021, from https://www.govinfo.gov/app/details/PLAW-104publ191; https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

Asswad, J., & Marx Gómez, J. (2021). Data ownership: a survey. . *Information., 12*(11)edux, 465.

Aun, J., Hurtado-Ram, D., Porras-D, L., Irigoyen-Pen, B., Rahmian, S., Al-Khazraji, Y., . . . Kotsev, A. (2024). Evaluation and Utilisation of Privacy Enhancing Technologies - A Data Spaces Perspective. *Data in Brief.* , 110560.

Awan, K. A., Din, I. U., Zareei, M., Talha, M., Guizani, M., & Jadoon, S. U. (2019). Holitrust-a holistic cross-domain trust management mechanism for service-centric Internet of Things. . *Ieee Access., 7*, 52191-52201.

Azad, M. A., Arshad, J., Mahmoud, S., Salah, K., & Imran, M. (2022). A privacy-preserving framework for smart context-aware healthcare applications. *Transactions on Emerging Telecommunications Technologies, 33*(8), e3634.

Azodo, I., Williams, R., Sheikh, A., & Cresswell, K. (2020). Opportunities and challenges surrounding the use of data from wearable sensor devices in health care: qualitative interview study. *Journal of Medical Internet Research., 22*(10), e19542.

Babu, S. B., & Jothi, K. R. (2024). A Secure Framework for Privacy-Preserving Analytics in Healthcare Records Using Zero-Knowledge Proofs and Blockchain in Multi-Tenant Cloud Environments. *IEEE Access.*

Bansal, S., & Kumar, D. (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *International Journal of Wireless Information Networks., 27*(3), 340-364.

Bansal, V., Baliyan, N., & Ghosh, M. (2024). MLChain: a privacy-preserving model learning framework using blockchain. International Journal of Information Security, 23(1), 649-677.

Barth, S. (2021). *Data, data, and even more data: Empowering users to make well-informed decisions about online privacy.* Enschede: University of Twente.

Becher, S., Gerl, A., Meier, B., & Bölz, F. (2020). Big picture on privacy enhancing technologies in e-health: a holistic personal privacy workflow. Information. *Information, 11*(7), 356.

Belguith, S., Kaaniche, N., Hammoudeh, M., & Dargahi, T. (2020). Proud: Verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted iot applications. *Future Generation Computer Systems., 11*, 899-918.

Bergram, K., Bezençon, V., Maingot, P., Gjerlufsen, T., & Holzer, A. (2020). Digital Nudges for Privacy Awareness: From consent to informed consent? *In Ecis.*

Bhadoria, R. K., Saha, J., Biswas, S., & Chowdhury, C. (2021). IoT-based location-aware smart healthcare framework with user mobility support in normal and emergency scenario: a comprehensive survey. *Healthcare Paradigms in the Internet of Things Ecosystem*, 137-161.

Bidgoli, H. (2023). Integrating Information Technology to Healthcare and Healthcare Management: Improving Quality, Access, Efficiency, Equity, and Healthy Lives. *American Journal of Management., 23*(3).

Boehme-Neßler, V. (2016). Privacy: a matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law., 6*(3), 222-229.

Boikanyo, K., Zungeru, A. M., Sigweni, B., Yahya, A., & Lebekwe, C. (2023). Remote patient monitoring systems: Applications, architecture, and challenges. . *Scientific African.*, e01638.

Bouijij, H., & Berqia, A. (2024). Enhancing IOT security: Proactive phishing website detection using Deep Neural Networks case study: smart home. *Journal of Telecommunications and the Digital Economy., 12*(1), 446-462.

Branscomb, A. W. (1994). *Who owns information? From privacy to public access.* Basic Books, Inc..

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health., 11*(4), 589-597.

Braun, V., & Clarke, V. (2021). One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology*, *18*(3), 328-352.

Braun, V., & Clarke, V. (2024). Thematic analysis. In *Encyclopedia of quality of life and well-being research* (pp. 7187-7193). Cham: Springer International Publishing.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). On privacy and security challenges in smart connected homes. . *In 2016 European Intelligence and Security Informatics Conference (EISIC). IEEE.*, 172 -175.

Bun, M., & Steinke, T. (2016). Concentrated differential privacy: Simplifications, extensions, and lower bounds. *In Theory of Cryptography Conference. Berlin, Heidelberg: Springer Berlin Heidelberg.*, 635-658.

Burkhardt, G., Boy, F., Doneddu, D., & Hajli, N. (2023). Privacy behaviour: A model for online informed consent. *Journal of business ethics., 186*(1), 237-255.

Bushwick, S. (2019, July 23). *"Anonymous" Data Won't Protect Your Identity.* Retrieved December 23, 2021, from https://www.scientificamerican.com/article/anonymous-data-wont-protect-your-identity/

Butun, I., Sari, A., & Österberg, P. (2019). Security implications of fog computing on the internet of things. *In 2019 IEEE International Conference on Consumer Electronics (ICCE) IEEE.*, 1 - 6.

Bygrave, L. A. (2017). Data protection by design and by default: deciphering the EU's legislative requirements. *Oslo Law Review., 4*(2), 105-120.

Cabrero-Holgueras, J., & Pastrana, S. (2021). Sok: Privacy-preserving computation techniques for deep learning. *Proceedings on Privacy Enhancing Technologies.*

Cardoso, E. O. (2023). *Privacy-by-design attribution model: a relative weight and spillover effect approach.* São Paulo: Universidade de São Paulo.

Carroll, S., Garba, I., Figueroa-Rodríguez, O., Holbrook, J., Lovett, R., Materechera, S., Sara, R. (2020). The CARE principles for indigenous data governance. *Data science journal.*, 19.

Cawthra, J., Cawthra, J., Grayson, N., Pulivarti, R., Hodges, B., Kuruvilla, J., Zheng, K. (2022). Securing telehealth remote patient monitoring ecosystem. *US Department of Commerce, National Institute of Standards and Technology.*

Ceccacci, S., & Mengoni, M. (2017). Designing smart home interfaces: traditional vs virtual prototyping. *In Proceedings of the 10th International Conference on PErvasive Technologies Related to Assistive Environments*, 67-74.

Chakraborty, A., Islam, M., Shahriyar, F., Islam, S., Zaman, H. U., & Hasan, M. (2023). Smart home system: a comprehensive review. *Journal of Electrical and Computer Engineering. , 2023*(1), 7616683.

Chang, S. E., Chen, Y., Lu, M., & Luo, H. L. (2020). Development and evaluation of a smart contract–Enabled blockchain system for home care service innovation: Mixed methods study. *JMIR medical informatics., 8*(7), e15472.

Chee, S. Y. (2024). Age-related digital disparities, functional limitations, and social isolation: unraveling the grey digital divide between baby boomers and the silent generation in senior living facilities. *Aging & mental health, 28(4), 28*(4), 621-632.

Chen, B., Tang, B., Guo, S., Yang, J., & Xiang, T. (2022). A Blockchain-Based Mutual Authentication Protocol for Smart Home. *In International Conference on Information Security. Cham: Springer International Publishing.*, 250-265.

Chen, C. Y., & Huang, J. J. (2023). Temporal-Guided Knowledge Graph-Enhanced Graph Convolutional Network for Personalized Movie Recommendation Systems. *Future Internet, 15*(10), 323.

Chen, F., Luo, Y., Zhang, J., Zhu, J., Zhang, Z., Zhao, C., & Wang, T. (2018). An infrastructure framework for privacy protection of community medical internet of things: Transmission protection, storage protection and access control. *World Wide Web., 21*, 33-57.

Chen, G., Zeng, F., Zhang, J., Lu, T., Shen, J., & Shu, W. (2021). An adaptive trust model based on recommendation filtering algorithm for the Internet of Things systems. *Computer Networks., 190*, 107952.

Chen, J., Edwards, L., Urquhart, L., & McAuley, D. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *International Data Privacy Law., 10*(4), 279-293.

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access, 7*, 74361-74382.

Chhetri, C., & Genaro Motti, V. (2022). User-centric privacy controls for smart homes. *Proceedings of the ACM on Human-Computer Interaction., 6*(CSCW2), 1-36.

Chibuike, M. C., Sara, G. S., & Adele, B. (2024). Overcoming challenges for improved patient-centric care: a scoping review of platform ecosystems in healthcare. *IEEE Access.*

Chiruvella, V., & Guddati, A. K. (2021). Ethical issues in patient data ownership. . *Interactive journal of medical research., 10*(2), e22269.

Cohen, J. (2013). Statistical power analysis for the behavioral sciences (2nd ed.). *Routledge. https://doi.org/10.4324/9780203771587*.

Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L.F. and Sadeh, N. (2020). Informing the design of a personalized privacy assistant for the internet of things. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems.*, 1 - 13.

Conley, J., Snyder, G. D., Whitehead, D., & Levine, D. M. (2022). Technology-enabled hospital at home: innovation for acute care at home. *NEJM Catalyst Innovations in Care Delivery. CAT-21., 3*(3), 21.

Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Glover, K., Haddadi, H., Wang, L. (2018). Building accountability into the Internet of Things: The IoT Databox model. *Journal of Reliable Intelligent Environments., 4*, 39-55.

Crutzen, R., Ygram Peters, G. J., & Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. *Psychology & Health., 34*(11), 1347-1357.

Culnane, C., Rubinstein, B. I., & Teague, V. (2017). Health data in an open world. . *arXiv preprint arXiv*, 712.05627.

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y. A., & Bourka, A. (2015). Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics. *arXiv preprint arXiv:1512.06000.*

Dankar, F. K., & El Emam, K. (2013). Dankar, F. K., & El Emam, K. (2013). Practicing differential privacy in health care: A review. . *Transaction on Data Privacy., 6*(1), 35-67.

Davis, M., Kirwan, M., Maclay, W., & Pappas, H. (. (2022). Closing the care gap with wearable devices: Innovating healthcare with wearable patient monitoring. *CRC Press.*

Demiris, G., & Thompson, H. (2011). Smart Homes and Ambient Assisted Living Applications: From Data to KnowledgeEmpowering or Overwhelming Older Adults?. *Yearbook of medical informatics., 20*(01), 51-57.

Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: a solution to secure IoT. *Wireless Personal Communications., 112*(3), 1947-1980.

Dhanraj, T., Kumar, M., Singh, S., Kumar, R., Jaiswal, P., & Mohapatra, H. (2024). A Review on Mitigating Privacy Risks in IoT-Enabled Smart Homes. *Computer Networks and Communications*, 146-163.

Di Sutam, E., Pei, F.L., Jia, J.T., Muhammad, N.A., Ab-Samat, H., Jeng, F.C., Prakash, J., Muhammad, N. & Sirivongpaisal, N., 2024. A comparative study on user satisfaction from manual to online information system using define-measure-analyze-improve-control (dmaic) in service administrative process. *Journal of Advanced Research Design*, *122*(1), pp.27-45.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States.*European Journal of Information Systems., 15*(4), 389-402.

Diraco, G., Rescio, G., Caroppo, A., Manni, A., & Leone, A. (2023). Human action recognition in smart living services and applications: context awareness, data availability, personalization, and privacy. *Sensors, 23*(13), 6040.

Dutta, S., Chukkapalli, S. S., Sulgekar, M., Krithivasan, S., Das, P. K., & Joshi, A. (2020). Context sensitive access control in smart home environments. *In 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). IEEE.*, 35-41.

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors., 19*(2), 326.

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science., 9*((3-4)), 211- 407.

Edemekong, P. F., Annamaraju, P., & Haydel, M. J. (2018). Health Insurance Portability and Accountability Act. *Europe-PMC*(https://europepmc.org/article/NBK/nbk500019). Retrieved from https://europepmc.org/article/NBK/nbk500019

Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal., 8*(14), 11717-11731.

El-Gendy, S., Elsayed, M. S., Jurcut, A., & Azer, M. A. (2023). Privacy preservation using machine learning in the internet of things. *Mathematics, 11*(16), 3477.

El Majdoubi, D., El Bakkali, H., Sadki, S., Maqour, Z., & Leghmid, A. (2022). *Security and Communication Networks., 1*, 5642026.

El Majdoubi, D., El Bakkali, H., Sadki, S., Maqour, Z., & Leghmid, A. (2022). The Systematic Literature Review of Privacy-Preserving Solutions in Smart Healthcare Environment. *Security and Communication Networks., 1*, 5642026.

EUR-Lex. (2016, May 04). *Access to European Union :aw.* Retrieved February 20, 2021, from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Famá, F., Faria, J. N., & Portugal, D. (2022). An IoT-based interoperable architecture for wireless biomonitoring of patients with sensor patches. *Internet of Things., 19*, 100547.

Fang, W., Zhu, C., Ma, T. M., Zhang, W., Li, B., Yi, L., . . . Wang, B. (2021). Dynamic aging weight scheme for trust model in Internet of Medical Things. *In 2021 IEEE International Conference on Bioinformatics and Biomedicine (BIBM) IEEE.*, 3366-3369.

Favaretto, M., De Clercq, E., & Elger, B. S. (2019). Big Data and discrimination: perils, promises and solutions. A systematic review. *Journal of Big Data., 6*(1), 1 - 27.

Felber, N. A., Tian, Y. J., Pageau, F., Elger, B. S., & Wangmo, T. (2023). Mapping ethical issues in the use of smart home health technologies to care for older persons: a systematic review. *BMC Medical Ethics., 24*(1), 24.

Firouzi, F., Chakrabarty, K., & Nassif, S. (2020). Healthcare IoT - Intelligent Internet of Things: From Device to Fog and Cloud, *Springer International Publishing.*(https://doi.org/10.1007/978-3-030-30367-9_11), 515-545.

Fox, J., Donnellan, A., & Doumen, L. (2019). The deployment of an IoT network infrastructure, as a localised regional service. *In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE.*, 319-324.

Gall, V. N., Buchhalter, J., Antonelli, R. C., Richard, C., Yohemas, M., Lachuk, G., & Gibbard, W. B. (2022). Improving care for families and children with neurodevelopmental disorders and co-occurring chronic health conditions using a care coordination intervention. *Journal of Developmental & Behavioral Pediatrics, 43*(8), 444-453.

Gao, W., & Zhou, S. (2023). Privacy-Preserving for Dynamic Real-Time Published Data Streams Based on Local Differential Privacy. *IEEE Internet of Things Journal.*

GeeksforGeeks. (2024, July 25). *5 Layer Architecture of Internet of Things.* Retrieved from GeeksforGeeks.org: https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. *In Artificial intelligence in healthcare. Academic Press.*, 295-336.

Ghosh, N., Chandra, S., Sachidananda, V., & Elovici, Y. (2019). SoftAuthZ: a context-aware, behavior-based authorization framework for home IoT. *IEEE Internet of Things Journal., 6*(6), 10773-10785.

Giordano, C., Brennan, M., Mohamed, B., Rashidi, P., Modave, F., & Tighe, P. (2021). Accessing artificial intelligence for clinical decision-making. . *Frontiers in digital health., 3*, 645232.

Gkoulalas-Divanis, A., & Loukides, G. S. (2014). Publishing data from electronic health records while preserving privacy: A survey of algorithms. *Journal of biomedical informatics., 50*, 4 -19.

Gomez-Trujillo, A. M., Velez-Ocampo, J., & Gonzalez-Perez, M. A. (2021). Trust, transparency, and technology: blockchain and its relevance in the context of the 2030 agenda. *The Palgrave Handbook of Corporate Sustainability in the Digital Era.*, 561-580.

Gong, Q., Zhang, J., Wei, Z., Wang, X., Zhang, X., Yan, X., Dong, L. (2024). SDACS: Blockchain-Based Secure and Dynamic Access Control Scheme for Internet of Things. *Sensors., 24*(7), 2267.

Gross, M. S., & Miller Jr, R. C. (2019). Ethical implementation of the learning healthcare system with blockchain technology. *Blockchain in Healthcare Today, Forthcoming*(http://dx.doi.org/10.2139/ssrn.3391034).

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems,, 29*(7), 1645-1660.

Gudala, L., Shaik, M., Venkataramanan, S., & Sadhu, A. K. (2019). Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT Networks. *Distributed Learning and Broad Applications in Scientific Research, 5*, 23-54.

Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling., 58*(5-6), 1189-1205.

HaddadPajouh, H., Khayami, R., Dehghantanha, A., Choo, K. K., & Parizi, R. M. (2020). AI4SAFE-IoT: An AI-powered secure architecture for edge layer of Internet of things. *Neural Computing and Applications, , 32*(20), 16119-16133.

Hammi, B., Zeadally, S., Khatoun, R., & Nebhen, J. (2022). Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Computers & Security. , 117*, 102677.

Hang, L., Kim, B., Kim, K., & Kim, D. (2021). A permissioned blockchain-based clinical trial service platform to improve trial data transparency. . *BioMed research international.*

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. . *Computer Communications., 153*, 311-335.

Heijsters, F. A., van Loon, G. A. P., Santema, J. M., Mullender, M. G., Bouman, M., de Bruijne, M. C., & van Nassau, F. (2023). A usability evaluation of the perceived user friendliness, accessibility,

and inclusiveness of a personalized digital care pathway tool. *International Journal of Medical Informatics*, *175*, 105070.

Hernandez, M. (2021). Enhancing Patient Care through Electronic Health Records (EHR) Systems. *Academic Journal of Science and Technology., 4*(1), 1-9.

Holvast, J. (2009). History of privacy. . *In The history of information security. Elsevier Science BV.*, 737-769.

Hommel, B., & Frings, C. (2020). The disintegration of event files over time: Decay or interference?. . *Psychonomic Bulletin & Review., 27*, 751-757.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. . *Information & Communications Technology Law., 28*(1), 65-98.

Hossain, M. S. (2016). Patient state recognition system for healthcare using speech and facial expressions. *Journal of medical systems., 40*, 1 - 8.

Hossein, K. M., Esmaeili, M. E., Dargahi, T., Khonsari, A., & Conti, M. (2021). BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. *Computer Communications*, *180*, 31-47.

Houser, K., & Bagby, J. W. (2023). Next-Generation Data Governance. *Duke Law & Technology Review.*

Hummel, P., Braun, M., & Dabrock, P. (2021). Own data? Ethical reflections on data ownership. . *Philosophy & Technology., 34*(3), 545-572.

Husnoo, M. A., Anwar, A., Chakrabortty, R. K., Doss, R., & Ryan, M. J. (2021). Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. *IEEE Access., 9*, 153276-153304.

Impiö, M., Yamaç, M., & Raitoharju, J. (2021, June). Multi-level reversible encryption for ECG signals using compressive sensing. In *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 1005-1009). IEEE.

Insights, F. B. (2024, November 25). *Hardware & Software IT Services - Smart Home Market.* Retrieved from https://www.fortunebusinessinsights.com/: https://www.fortunebusinessinsights.com/industry-reports/smart-home-market-101900

Iqbal, W., Abbas, H., Rauf, B., Bangash, Y. A., Amjad, M. F., & Hemani, A. (2021). PCSS: privacy preserving communication scheme for SDN enabled smart homes. *IEEE Sensors Journal, 22(18), , 22*(18), 17677-17690.

Irshad, R., Sohail, S., Hussain, S., Madsen, D., Ahmed, M., Alattab, A., . . . Ahmed, A. (2023). A multi-objective bee foraging learning-based particle swarm optimization algorithm for enhancing the security of healthcare data in cloud system. *IEEE Access., 11*, 113410-113421.

Islam, S. M., Bari, M. S., Sarkar, A., Obaidur, A., Khan, R., & Paul, R. (2024). AI-driven threat intelligence: Transforming cybersecurity for proactive risk management in critical sectors. *International Journal of Computer Science and Information Technology, 16*(5), 125 - 131.

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. *In 2020 IEEE*

International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) IEEE., 310-317.

Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors., 23*(21), 8944.

James, E., & Rabbi, F. (2023). Fortifying the IoT landscape: Strategies to counter security risks in connected systems. *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries., 6*(1), 32 - 46.

Janssen, H., Cobbe, J., Norval, C., & Singh, J. (2020). Decentralized data processing: personal data stores and the GDPR. *International Data Privacy Law., 10*(4), 356-384.

Jarin, I., & Eshete, B. (2022). Dp-util: Comprehensive utility analysis of differential privacy in machine learning. *In Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy.*, 41-52.

Jayaraman, B., & Evans, D. (2019). *In 28th USENIX Security Symposium (USENIX Security 19)*, 1895-1912.

Jayaraman, B., & Evans, D. (2019). *In 28th USENIX Security Symposium (USENIX Security 19)*, 1895-1912.

Jeyaraman, M., Balaji, S., Jeyaraman, N., & Yadav, S. (2023). Unraveling the ethical enigma: artificial intelligence in healthcare. *Cureus, 15*(8).

Jiang, J., Wang, H., & Li, W. (2020). A Trust model based on a time decay factor for use in social networks. *Computers & Electrical Engineering., 85*, 106706.

Jiang, R., Liu, R., Zhang, T., Ding, W., & Tian, S. (2024). An electronic medical record access control model based on intuitionistic fuzzy trust. *Information Sciences, 658*, 120054.

Jo, T. H., Ma, J. H., & Cha, S. H. (2021). Elderly perception on the internet of things-based integrated smart-home system. *Sensors, 21*(4), 1284.

Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. *IEEE Internet Computing., 25*(4), 37- 48.

Kassab, W. A., & Darabkh, K. A. (2020). A–Z survey of internet of things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications., 163*, 102663.

Kaundinya, T., & Agrawal, R. (2022). Unpacking a telemedical takeover: recommendations for improving the sustainability and usage of telemedicine post-COVID-19. *Quality Management in Healthcare., 31*(2), 68-73.

Kaya, A., Ozturk, R., & Altin Gumussoy, C. (2019). Usability measurement of mobile applications with system usability scale (SUS). In *Industrial Engineering in the Big Data Era: Selected Papers from the Global Joint Conference on Industrial Engineering and Its Application Areas, GJCIE 2018, June 21–22, 2018, Nevsehir, Turkey* (pp. 389-400). Springer International Publishing.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal., 25*(6), 607 -635.

Keulen, S., & Kroeze, R. (2018). Privacy from a historical perspective. *The handbook of privacy studies: An interdisciplinary introduction.*, 21-56.

Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine., 158*, 106848.

Khanna, S., & Srivastava, S. (2020). Patient-centric ethical frameworks for privacy, transparency, and bias awareness in deep learning-based medical systems. *Applied Research in Artificial Intelligence and Cloud Computing., 3*(1), 16-35.

Khanpara, P., Lavingia, K., Trivedi, R., Tanwar, S., Verma, A., & Sharma, R. (2023). A context-aware internet of things-driven security scheme for smart homes. *Security and Privacy, 6*(1), e269.

Khilnani, A., Schulz, J., & Robinson, L. (2020). The COVID-19 pandemic: new concerns and connections between eHealth and digital inequalities. *Journal of Information, Communication and Ethics in Society. , 18*(3), 393- 403.

Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A review of insider threat detection approaches with IoT perspective. *IEEE Access, 8*, 78847-78867.

Kim, T. M., Lee, S. J., Chang, D. J., Koo, J., Kim, T., Yoon, K. H., & Choi, I. Y. (2021). DynamiChain: development of medical blockchain ecosystem based on dynamic consent system. *Applied Sciences,., 11*(4), 1612.

Kolain, M., & Wirth, C. (2018). Privacy by BlockChain Design: A blockchain-enabled GDPR-compliant approach for handling personal data. *In Blockchain Engineering: Challenges and Opportunities for Computer Science Research. Proceedings of the 1st ERCIM Blockchain Workshop, 8-9 May 2018,European Society for Socially Embedded Technologies (EUSSET).* Amsterdam, Netherlands.

Kounoudes, A. D., & Kapitsaki, G. M. (2020). A mapping of IoT user-centric privacy-preserving approaches to the GDPR. *Internet of Things., 11*, 100179.

Kshetri. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027–1038.

Kumar, A., Braud, T., Kwon, Y. D., & Hui, P. (2020). Aquilis: Using contextual integrity for privacy protection on mobile devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies., 4*(4), 1 - b28.

Kumar, M., & Chand, S. (2020). A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability. *IEEE Internet of Things Journal., 7*(10), 10650-10659.

Kumar, S., Underwood, S. H., Masters, J. L., Manley, N. A., Konstantzos, I., Lau, J., Wang, L. M. (2023). Ten questions concerning smart and healthy built environments for older adults. *Building and Environment., 244*, 110720.

Lavanya, M., & Kavitha, V. (2022). Secure tamper-resistant electronic health record transaction in cloud system via blockchain. *Wireless Personal Communications., 124*(1), 607-632.

Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Communications Surveys & Tutorials., 23*(2), 1020-1047.

Lee, H., & Kobsa, A. (2016). Understanding user privacy in internet of things environments. *In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE.*, 407- 412.

Lee, H., & Kobsa, A. (2017). Privacy preference modeling and prediction in a simulated campuswide IoT. *In 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE.*, 276-285.

Lee, S. W. (2022). Methods for testing statistical differences between groups in medical research: statistical standard and guideline of Life Cycle Committee. *Life Cycle*, *2*.

Lefkovitz, N., & Boeckl, K. (2020). *NIST Privacy Framework: An Overview.* Retrieved February 28, 2021, from https://tsapps.nist.gov/publication/getpdf.cfm?pub id=930470

Li, W., Li, Y., Zheng, C., & He, R. (2023, August). Blockchain-based Model for Privacy-enhanced Data Sharing. In *2023 10th International Conference on Dependable Systems and Their Applications (DSA)* (pp. 406-417). IEEE.

Li, W., Yigitcanlar, T., Erol, I., & Liu, A. (2021). Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. *Energy Research & Social Science., 80*, 102211.

Li, W., Yigitcanlar, T., Liu, A., & Erol, I. (2022). Mapping two decades of smart home research: A systematic scientometric analysis. *Technological Forecasting and Social Change., 179*, 121676.

Liew, M. S., Zhang, J., See, J., & Ong, Y. L. (2019). Usability challenges for health and wellness mobile apps: mixed-methods study among mHealth experts and consumers. *JMIR mHealth and uHealth*, *7*(1), e12160.

Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., & Choo, K. K. (2019). HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal., 7*(2), 818-829.

Liu, G., Zhang, R., Wan, B., Ji, S., & Tian, Y. (2020). Extended Role-Based Access Control with Context-Based Role Filtering. *KSII Transactions on Internet and Information Systems (TIIS)., 14*(3), 1263-1279.

Liu, Y., Ouyang, D., Liu, Y., & Chen, R. (2017). A novel approach based on time cluster for activity recognition of daily living in smart homes. *Symmetry., 9*(10), 212.

Luo, E., Bhuiyan, M. Z., Wang, G., Rahman, M. A., Wu, J., & Atiquzzaman, M. (2018). Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Communications Magazine., 56*(2), 163-168.

Luo, X., Tan, H., & Wen, W. (2024). Recent Advances in Wearable Healthcare Devices: From Material to Application. *Bioengineering., 11*(4), 358.

Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. *In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 254 - 269.

Ma, J., Naas, S. A., Sigg, S., & Lyu, X. (2022). Privacy-preserving federated learning based on multi-key homomorphic encryption. . *International Journal of Intelligent Systems., 37*(9), 5880-5901.

Mackey, T., Kuo, T., Gummadi, B., Clauson, K., Church, G., Grishin, D., Palombini, M. (2021). Fit-for-purpose?—challenges and opportunities for applications of blockchain technology in the future of healthcare. *Advances in Clinical Immunology, Medical Microbiology, COVID-19, and Big Data, 17*, 583-609.

Mahdi, M. S., Hassan, N. F., & Abdul-Majeed, G. H. (2021). An improved chacha algorithm for securing data on IoT devices. *SN Applied Sciences, 3*(4), 1-9.

Mahmmod, B., Naser, M., Al-Sudani, A., Alsabah, M., Mohammed, H., Alaskar, H., Abdulhussain, S. (2024). Patient monitoring system based on internet of things: A review and related challenges with open research issues. *IEEE Access.*

Majeed, A., & Lee, S. (2020). Anonymization techniques for privacy preserving data publishing: A comprehensive survey. *IEEE access., 9*, 8512-8545.

Majumder, S., Aghayi, E., Noferesti, M., Memarzadeh-Tehran, H., Mondal, T., Pang, Z., & Deen, M. J. (2017). Smart homes for elderly healthcare—Recent advances and research challenges. *Sensors., 17*(11), 2496.

Maleh, Y., Shojafar, M., Alazab, M., & Romdhani, I. (2020). *Blockchain for cybersecurity and privacy: architectures, challenges, and applications.* Google Books: CRC Press, Yaylor & Francis Croup.

Malik, S., & Shah, M. A. (2022). Access Control using Blockchain: A Taxonomy and Review. *In Proceedings of the 6th International Conference on Information System and Data Mining.*, 46-54.

Mamo, N., Martin, G. M., Desira, M., Ellul, B., & Ebejer, J. P. (2020). Dwarna: a blockchain solution for dynamic consent in biobanking. *European Journal of Human Genetics., 28*(5), 609-626.

Masmoudi, A., & Saeed, M. (2024). Blockchain-Driven Decentralization of Electronic Health Records in Saudi Arabia: An Ethereum-Based Framework for Enhanced Security and Patient Control. *International Journal of Advanced Computer Science & Applications., 15*(4).

Mazumdar, S., & Dreibholz, T. (2022). Secure Embedded Living: Towards A Self-Contained User Data Preserving Framework. . *IEEE Communications Magazine., 60*(11), 74 -80.

Mbunge, E., Muchemwa, B., & Batani, J. (2021). Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies. *Global Health Journal, 5*(4), 169-177.

Mehta, V., Gooch, D., Bandara, A., Price, B., & Nuseibeh, B. (2021). Privacy care: A tangible interaction framework for privacy management. . *ACM Transactions on Internet Technology (TOIT), 21*(1), 1-32.

Melnikovas, A. (2018). Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies. *Journal of futures Studies, 23*(2).

Merlec, M. M., Lee, Y. K., Hong, S. P., & In, H. P. (2021). A smart contract-based dynamic consent management system for personal data usage under GDPR. . *Sensors., 21*(23), 7994.

Miao, G., Ding, A. A., & Wu, S. S. (2022). Real-time privacy preserving disease diagnosis using ECG signal. *arXiv preprint arXiv:2202.03652*.

Miranda-Pascual, À., Guerra-Balboa, P., Parra-Arnau, J., Forné, J., & Strufe, T. (2023). Miranda-Pascual, À., Guerra-Balboa, P., Parra-Arnau, J., Forné, J., & Strufe, T. (2023). SoK: Differentially private publication of trajectory data. . *Proceedings on Privacy Enhancing Technologies.*

Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access., 9*, 59353-59377.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society., 3*(2), 2053951716679679.

Mohammed, M. N., Desyansah, S. F., Al-Zubaidi, S., & Yusuf, E. (2020). An internet of things-based smart homes and healthcare monitoring and management system. *In Journal of physics: conference series. IOP Publishing., 1450*(1), 012079.

Mohebbi, A., & Pouilly, L. (2020, June 8). *The Offboarding User Experience: A Comparative Study.* Retrieved from UX Matters: https://www.uxmatters.com/mt/archives/2020/06/the-offboarding-user-experience-a-comparative-study.php

Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science., 52*, 452-459.

Morita, P. P., Sahu, K. S., & Oetomo, A. (2023). Health monitoring using smart home technologies: Scoping review. *JMIR mHealth and uHealth., 11*, e37347.

Morrison, J. (2016). Context integrity measurement architecture: a privacy-preserving strategy for the era of ubiquitous computing. *In 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE.*, 1 - 10.

Mosquera-Lopez, C., Wan, E., Shastry, M., Folsom, J., Leitschuh, J., Condon, J., . . . Jacobs, P. (2020). Automated detection of real-world falls: Modeled from people with multiple sclerosis. *IEEE journal of biomedical and health informatics., 25*(6), 1975-1984.

Motti, V. G., & Berkovsky, S. (2022). Healthcare privacy. *In Modern Socio-Technical Perspectives on Privacy. Cham: Springer International Publishing* , 203-231.

Muravyeva, E., Janssen, J., Specht, M., & Custers, B. (2020). Exploring solutions to the privacy paradox in the context of e-assessment: Informed consent revisited. *Ethics and Information Technology., 23*(3), 223-238.

Murphy, E., Gordon, D., Keegan, B., Doyle, J., Stavrakakis, I., & O'Sullivan, D. (2022). Towards an Ethical Framework for the Design and Development of Inclusive Home-based Smart Technology for Older Adults and People with Disabilities. . *HEALTHINF*, 614-622.

Nasir, M., Muhammad, K., Ullah, A., Ahmad, J., Baik, S. W., & Sajjad, M. (2022). Enabling automation and edge intelligence over resource constraint IoT devices for smart home. *Neurocomputing., 491*, 494-506.

Neisse, R., Steri, G., & Nai-Fovino, I. (2017). A blockchain-based approach for data accountability and provenance tracking. *In Proceedings of the 12th international conference on availability, reliability and security*, (pp. 1-10).

Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare., 2*(3), 1 - 44.

Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. *In The ethics of information technologies. Routledge.*, 141-178.

Nunnally, J., & Bernstein, I. (1994). *Psychometric Theory 3rd edition.* New York: MacGraw-Hill.

OAG. (2018, July 31). *California Consumer Privacy Act (CCPA).* Retrieved February 23, 2021, from https://www.oag.ca.gov/privacy/ccpa

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review., 38*, 100312.

OPC. (2019, June 21). *PIPEDA fair information principles.* Retrieved February 21, 2021, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Osasona, F., Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., & Ayinla, B. S. (2024). Reviewing the ethical implications of AI in decision making processes. *International Journal of Management & Entrepreneurship Research., 6*(2), 322-335.

Osman, L., Taiwo, O., Elashry, A., & Ezugwu, A. E. (2023). Intelligent Edge Computing for IoT: Enhancing Security and Privacy. *Journal of Intelligent Systems & Internet of Things., 8*(1).

Othman, S. B., Almalki, F. A., Chakraborty, C., & Sakli, H. (2022). Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies. *Computers and Electrical Engineering, 101*, 108025.

Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. *Advances in Intelligent Systems and Computing, 520*, 523-533.

Outchakoucht, A., Hamza, E. S., & Leroy, J. P. (2017). Dynamic access control policy based on blockchain and machine learning for the internet of things. *International journal of advanced Computer Science and applications., 8*(7).

Oyeniyi, J., & Oluwaseyi, P. (2024). Emerging Trends in AI-Powered Medical Imaging: Enhancing Diagnostic Accuracy and Treatment Decisions. *International Journal of Enhanced Research in Science, Technology & Engineering, 13*(4), 2319-7463.

Park, S., Lenhart, A., Zimmer, M., & Vitak, J. (2023). Nobody's Happy": Design Insights from {Privacy-Conscious} Smart Home Power Users on Enhancing Data Transparency, Visibility, and Control. *In Nineteenth Symposium on Usable Privacy and Security (SOUPS).*

Parkinson, S., & Khan, S. (2022). A survey on empirical security analysis of access-control systems: a real-world perspective. *ACM Computing Surveys, 55*(6), 1 - 28.

Parvathy, V. S., Pothiraj, S., & Sampson, J. (2021). Automated internet of medical things (IoMT) based healthcare monitoring system. *Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications.*, 117-128.

Patel, N. J., & Jadhav, A. (2024). Design of an efficient dynamic context-based privacy policy deployment model via dual bioinspired Q learning optimisations. *IET Cyber-Physical Systems: Theory & Applications.*

Patel, O., & Patel, H. (2023). IBLOSH: IOT-Enabled Blockchain-Based Data Security Framework for Healthcare System. *International Journal of Intelligent Systems and Applications in Engineering., 11*(3), 1240-1250.

Patil, S., Joshi, S., & Patil, D. (2020). Enhanced privacy preservation using anonymization in IoT-enabled smart homes. *In Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics. Springer Singapore., 1*, 439-454.

Pavlović, N., Šarac, M., Adamović, S., Saračević, M., Ahmad, K., Maček, N., & Sharma, D. K. (2022). An approach to adding simple interface as security gateway architecture for IoT device. *Multimedia Tools and Applications., 81*(26), 36931-36946.

Peng, S. Y. (2022). Public–Private Interactions in Privacy Governance. *Laws., 11*(6), 80.

Pham, H. L., Tran, T. H., & Nakashima, Y. (2018). A secure remote healthcare system for hospital using blockchain smart contract. *In 2018 IEEE globecom workshops (GC Wkshps) IEEE.*, 1 -6.

Pirzada, P., Wilde, A., Doherty, G. H., & Harris-Birtill, D. (2022). Ethics and acceptance of smart homes for older adults. *Informatics for Health and Social Care., 47*(1), 10-37.

Ploug, T., & Holm, S. (2020). The four dimensions of contestable AI diagnostics-A patient-centric approach to explainable AI. *Artificial Intelligence in Medicine., 107*, 101901.

Popoola, O., Rodrigues, M. A., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). An Optimized Hybrid Encryption Framework for Smart Home Healthcare: Ensuring Data Confidentiality and Security. *Internet of Things.*, 101314.

Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehia, A., & Popoola, J. (2023). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions. *Blockchain: Research and Applications.*, 100178.

Pradhan, N.R., Singh, A.P., Verma, S., Kavita, Kaur, N., Roy, D.S., Shafi, J., Wozniak, M. and Ijaz, M.F., 2022. A novel blockchain-based healthcare system design and performance benchmarking on a multi-hosted testbed. *Sensors*, *22*(9), 3449.

Prange, S., Shams, A., Piening, R., Abdelrahman, Y., & Alt, F. (2021). Priview–exploring visualisations to support users' privacy awareness. *In Proceedings of the 2021 chi conference on human factors in computing systems.*, 1 - 18.

Prastio, W. T., & Sugiharto, A. (2024). Comparative Analysis of User Satisfaction of End User Computing Satisfaction, DeLone & McLean and Webqual 4.0 Methods. *Jurnal Penelitian Pendidikan IPA*, *10*(9), 6826-6834.

Prathik, A., Banu, S. P., Sagar, B. S., Prakash, A. J. F., Thamizhamuthu, R., & Velmurugan, S. (2024,

October). Telehealth Data Security and Privacy Solutions for Sensitive Health Records using Cloud Computing and Isolation Forest Algorithm. In *2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)* (pp. 1199-1204). IEEE.

Psychoula, I. (2020). *Privacy Modelling and Preservation for Assisted Living within Smart Homes.* Thesis, De Montfort University Leicester.

Psychoula, I., Chen, L., & Amft, O. (2020). *Privacy Risk Awareness in Wearables and the Internet of Things. IEEE Pervasive Computing., 19*(3), 60-66.

Psychoula, I., Chen, L., Yao, X., & Ning, H. (2019). A privacy aware architecture for IoT enabled systems. *In 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) IEEE*, 178-183.

Psychoula, I., Merdivan, E., Singh, D., Chen, L., Chen, F., Hanke, S., Kropf, J., Holzinger, A. and Geist, M., 2018, March. A deep learning approach for privacy preservation in assisted living. In *2018 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops)* (pp. 710-715). IEEE.

Psychoula, I., Singh, D., Chen, L., Chen, F., Holzinger, A., & Ning, H. (2018). Users' Privacy Concerns in IoT Based Applications. *In The 4th IEEE International Conference on Internet of People*.

Pujari, C., Muniyal, B., Rao, A., Sadiname, V., & Rajarajan, M. (2023). Identity resilience in the digital health ecosystem: A key recovery-enabled framework. *Computers in Biology and Medicine*, *167*, 107702.

Pu, X., Jiang, R., Song, Z., Liang, Z., & Yang, L. (2024). A medical big data access control model based on smart contracts and risk in the blockchain environment. *Frontiers in Public Health., 12*, 1358184.

Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., & Kim, S. W. (2020). The future of healthcare internet of things: a survey of emerging technologies. *IEEE Communications Surveys & Tutorials., 22*(2), 1121-1167.

Qing, H., Ibrahim, R., & Nies, H. W. (2024). Context-aware Location Privacy Protection Method. . *Baghdad Science Journal.*

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *ournal of the Academy of Marketing Science., 50*(6), 299-1323.

Qu, X., Yang, Z., Chen, Z., & Sun, G. (2025). A consent-aware electronic medical records sharing method based on blockchain. *Computer Standards & Interfaces*, *92*, 103902.

Rafique, W., Khan, M., Khan, S., & Ally, J. S. (2023). SecureMed: A Blockchain-Based Privacy-Preserving Framework for Internet of Medical Things. *Wireless Communications and Mobile Computing., 1*, 2558469.

Ragothaman, K., Wang, Y., Rimal, B., & Lawrence, M. (2023). Access control for IoT: A survey of existing research, dynamic policies and future directions. *Sensors., 23*(4), 1805.

Raghav, Y. Y., Choudhary, S., Pandey, P., Singh, S., & Varshney, D. (2025). Smart Healthcare: Cloud-IoT Solutions for Enhanced Patient Well-Being. *African Journal of Biomedical Research, 28*(1), 14 - 28.

Rahanu, H., Georgiadou, E., Siakas, K., Ross, M., & Berki, E. (2021). Ethical issues invoked by Industry 4.0. *In European Conference on Software Process Improvement. Springer, Cham.*, 589 -606.

Rahimi, M., Songhorabadi, M., & Kashani, M. H. (2020). Fog-based smart homes: A systematic review. *Journal of Network and Computer Applications*, *153*, 102531.

Rahman, M., Hasan, M., Rahman, M., & Momotaj, M. (2024). *A Framework for Patient-Centric Consent Management Using Blockchain Smart Contracts in Predictive Analysis for Healthcare Industry. International Journal of Health Systems and Medical Sciences., 3*(3), 45-59.

Rahmati, M. (2025). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities. *arXiv preprint arXiv:2502*, 10599.

Rajasekaran, A. S., Maria, A., Rajagopal, M., & Lorincz, J. (2023). Blockchain Enabled Anonymous Privacy-Preserving Authentication Scheme for Internet of Health Things. *Sensors., 23*(1), 240.

Rana, M. S., & Shuford, J. (2024). AI in Healthcare: Transforming Patient Care through Predictive Analytics and Decision Support Systems. *Journal of Artificial Intelligence General Science (JAIGS), 1*(1), 3006 - 4023.

Ranjan, A. K., & Kumar, P. (2024). Ensuring the privacy and security of IoT-medical data: a hybrid deep learning-based encryption and blockchain-enabled transmission. *Multimedia Tools and Applications.*, 1-26.

Rehan, H. (2024). The Future of Safeguarding Sensitive Data in the Digital Age. *Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023, 1*(1), 132-151.

Renukappa, S., Mudiyi, P., Suresh, S., Abdalla, W., & Subbarao, C. (2022). Evaluation of challenges for adoption of smart healthcare strategies. *Smart Health., 26*, 100330.

Research, BCC. (2018, December). *Global Smart Home Market.* Retrieved June 2021, from https://www.bccresearch.com/partners/verified-market-research/global-smart-home-market.html

Rhee, J. H., Ma, J. H., Seo, J., & Cha, S. H. (2022). Review of applications and user perceptions of smart home technology for health and environmental monitoring. *Journal of Computational Design and Engineering., 9*(3), 857-889.

Rifi, N., Agoulmine, N., Chendeb Taher, N., & Rachkidi, E. (2018). Blockchain technology: is it a good candidate for securing iot sensitive medical data? *Wireless Communications and Mobile Computing,*.

Rivadeneira, J. E., Silva, J. S., Colomo-Palacios, R., & Rodrigues, A. B. (2023). *User-centric privacy preserving models for a new era of the Internet of Things. Journal of Network and Computer Applications*, 103695.

Rivadeneira, J. E., Jiménez, M. B., Marculescu, R., Rodrigues, A., Boavida, F., & Sá Silva, J. (2023, May). A blockchain-based privacy-preserving model for consent and transparency in human-

centered Internet of Things. In *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation* (pp. 301-314).

Rocher, L., Hendrickx, J. M., & De Montjoye, Y. A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature communications., 10*(1), 1 - 9.

Rock, L. Y., Tajudeen, F. P., & Chung, Y. W. (2024). Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective. *Universal access in the information society., 23*(1), 345-364.

Rogers, C. K., Parulekar, M., Malik, F., & Torres, C. A. (2022). A local perspective into electronic health record design, integration, and implementation of screening and referral for social determinants of health. *Perspectives in health information management.*, 19.

Rossi, A., & Lenzini, G. (2020). Transparency by design in data-informed research: A collection of information design patterns. *Computer Law & Security Review., 37*, 105402.

Rovolis, G., & Habibipour, A. (2024). When participatory design meets data-driven decision making: A literature review and the way forward. *Management Science Letters., 14*(2), 107-126.

Rubeis, G. (2022). The ethics of artificial intelligence and big data in mental healthcare. *Internet Interventions., 28*, 100518.

Sahu, M., Gupta, R., Ambasta, R. K., & Kumar, P. (2022). Artificial intelligence and machine learning in precision medicine: A paradigm shift in big data analysis. *Progress in molecular biology and translational science. , 190*(1), 57-100.

Saifuzzaman, M., Ananna, T. N., Chowdhury, M. J., Ferdous, M. S., & Chowdhury, F. (2022). A systematic literature review on wearable health data publishing under differential privacy. *International Journal of Information Security., 21*(4), 847-872.

Salehi, A., Han, R., Rudolph, C., & Grobler, M. (2023). DACP: Enforcing a dynamic access control policy in cross-domain environments. *Computer Networks*, *237*, 110049.

Schomakers, E. M., & Ziefle, M. (2023). Privacy vs. security: trade-offs in the acceptance of smart technologies for aging-in-place. *International Journal of Human-Computer Interaction., 39*(5), 1043-1058.

Seuring, S., Stella, T., & Stella, M. (2021). Developing and publishing strong empirical research in sustainability management—Addressing the intersection of theory, method, and empirical field. *Frontiers in Sustainability, 1*, 617870.

Shah, J. L., Bhat, H. F., & Khan, A. I. (2021). Integration of cloud and IoT for smart e-healthcare. *In Healthcare paradigms in the internet of things ecosystem, Academic Press.*, 101-136.

Shahlaei, M., & Hashemi, S. M. (2024). A risk-aware and recommender distributed intrusion detection system for home robots. *Journal of Information Security and Applications., 83*, 103777.

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE access, 7*, 147782-147795.

Shahraki, A. S., Rudolph, C., & Grobler, M. (2019, August). A dynamic access control policy model for sharing of healthcare data in multiple domains. In 2019 18th IEEE International Conference

On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 618-625). IEEE.

Shang, Y. (2017). Studies on user intent analysis and mining. *Drexel University.*

Sharma, A. (2024). Demystifying Privacy-preserving AI: Strategies for Responsible Data Handling. *MZ Journal of Artificial Intelligence., 1*(1), 1 - 8.

Sharma, S., Chen, K., & Sheth, A. (2018). Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. *IEEE Internet Computing, 22*(2), 42-51.

Shrivastava, S., & Srikanth, T. K. (2023). A Comprehensive Consent Management System for Electronic Health Records in the Healthcare Ecosystem. *In Information Security and Privacy in Smart Devices: Tools, Methods, and Applications. IGI Global.*, 194-233.

Siddamsetti, S., Tejaswi, C., & Maddula, P. (2024). Anomaly detection in blockchain using machine learning. *Journal of Electrical Systems*, *20*(3), 619-634.

Siddiqui, S., Khan, A. A., & Dey, I. (2022). Internet Technologies for Personalized Care. *In Information and Communication Technology (ICT) Frameworks in Telehealth. Cham: Springer International Publishing.*, 173-189.

Sikder, A. K., Babun, L., Celik, Z. B., Aksu, H., McDaniel, P., Kirda, E., & Uluagac, A. S. (2022). Who's controlling my device? Multi-user multi-device-aware access control system for shared smart home environment. *ACM Transactions on Internet of Things., 3*(4), 1 - 39.

Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2021). A survey on sensor-based threats and attacks to smart devices and applications. *IEEE Communications Surveys & Tutorials., 23*(2), 1125-1159.

Silva, I., & Soto, M. (2022). Privacy-preserving data sharing in healthcare: an in-depth analysis of big data solutions and regulatory compliance. *International Journal of Applied Health Care Analytics., 7*(1), 14-23.

Silva, P., Gonçalves, C., Antunes, N., Curado, M., & Walek, B. (2022). Privacy risk assessment and privacy-preserving data monitoring. *Expert Systems with Applications., 200*, 116867.

Sim, J., Kim, B., Jeon, K., Joo, M., Lim, J., Lee, J., & Choo, K. K. R. (2023). Technical requirements and approaches in personal data control. *ACM Computing Surveys*, *55*(9), 1-30.

Singh, A., & Rathee, G. (2025). Smart contract empowered dynamic consent: decentralized storage and access control for healthcare applications. *Peer-to-Peer Networking and Applications*, *18*(1), 1-16.

Singh, C., Juneja, N., & Kaur, S. (2022). A Case Study of Trust Management for Authorization and Authentication in IoT Devices Using Layered Approach. *In Society 5.0 and the Future of Emerging Computational Technologies. CRC Press.*, 45 - 62.

Singh, R., Joshi, J., Goyal, A., Rathi, P., & Joshi, K. (2024, May). Security and Privacy Measures to Protect Machine Learning in Medical Applications. In *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)* (pp. 641-646). IEEE.

Singh, S., & Kumar, D. (2023). Energy-efficient secure data fusion scheme for IoT based healthcare system. *Future Generation Computer Systems., 143*, 15-29.

Sivakumar, C. L., Mone, V., & Abdumukhtor, R. (2024). Addressing privacy concerns with wearable health monitoring technology. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 14*(3), e1535.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review., 126*, 1880.

Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law.* Aspen Publishing.

Sousa, J., Mendonça, J. P., & Machado, J. (2022). A generic interface and a framework designed for industrial metrology integration for the Internet of Things. *Computers in Industry., 138*, 103632.

Soykan, E. U., Karacay, L., Karakoc, F., & Tomur, E. (2022). A survey and guideline on privacy enhancing technologies for collaborative machine learning. *IEEE Access., 10*, 97495-97519.

Sripathi, M., & Leelavati, T. S. (2024). The Fourth Industrial Revolution: A paradigm shift in healthcare delivery and management. *Digital Transformation in Healthcare 5.0: IoT, AI and Digital Twin., 1*(67).

Statista. (n.d.). *Internet of Things (IoT) connected devices installed worldwide.* Retrieved from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Suriyakumar, V. M., Papernot, N., Goldenberg, A., & Ghassemi, M. (2021). Chasing your long tails: Differentially private prediction in health care settings. *In Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency.*, 723-734.

Surya, V., Ranichandra, S., & Ranjani, R. (2018). Secure cloud storage using AES encryption. *International Journal of Innovative Research in Computer and Communication Engineering. , 6*(6), 6308-6312.

Sylla, T., Chalouf, M. A., Krief, F., & Samaké, K. (2021). Context-aware security in the internet of things: a survey. *International journal of autonomous and adaptive communications systems., 14*(3), 231-263.

Tabassum, M., Mahmood, S., Bukhari, A., Alshemaimri, B., Daud, A., & Khalique, F. (2024). Anomaly-based threat detection in smart health using machine learning. *BMC Medical Informatics and Decision Making*, *24*(1), 347.

Takale, D. G., Gawali, P. P., Deshmukh, G. B., Mahalle, P. N., Mehta, P. S., Kashid, S. S., ... & Derle, D. R. (2024, April). Enhancing Security and Privacy in Health Care Using Cyber-physical Systems Through Machine Learning. In *International Conference on Information and Communication Technology for Intelligent Systems* (pp. 395-408). Singapore: Springer Nature Singapore.

Tammina, M. R., Posinasetty, B., Nair, P. S., Kumar, S., Pavithra, G., & Kaur, H. (2024, April). Machine Learning Enabled Healthcare Balancing Patient Privacy and Data Utility. In *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)* (pp. 1-6). IEEE.

Tan, L., Shi, N., Yu, K., Aloqaily, M., & Jararweh, Y. (2021). A blockchain-empowered access control framework for smart devices in green internet of things. *ACM Transactions on Internet Technology (TOIT)., 21*(3), 1 - 20.

Tan, L., Yu, K., Shi, N., Yang, C., Wei, W., & Lu, H. (2021). Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach. *IEEE Transactions on Network Science and Engineering., 9*(1), 271-281.

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications, 50*, 102407.

Tasali, Q., Chowdhury, C., & Vasserman, E. Y. (2017). A flexible authorization architecture for systems of interoperable medical devices. *In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, 9 - 20.

Thangamani, R., Kamalam, G. K., & Vimaladevi, M. (2024). Revolutionizing Healthcare Processes: The Dynamic Role of Blockchain Innovation. In *Blockchain for Biomedical Research and Healthcare: Concept, Trends, and Future Implications* (pp. 229-267). Singapore: Springer Nature Singapore.

Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M., Taira, N., Obi, T., & Ohyama, N. (2020). Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. *Healthcare Informatics Research., 26*(4), 265-273.

Tiwari, V. K., & Singh, V. (2016). Study of Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *International Journal of Advanced Research in Computer Science., 7*(7).

Toni, M., Mattia, G., & Pratesi, C. A. (2024). What's next in the Healthcare system? The contribution of digital innovation in achieving Patient-centricity. *Futures., 156*, 103304.

Torre, D., Chennamaneni, A., & Rodriguez, A. (2023). Privacy-preservation techniques for IoT devices: a systematic mapping study. *IEEE Access, 11*, 16323-16345.

Trnka, M., Cerny, T., & Stickney, N. (2018.). Survey of Authentication and Authorization for the Internet of Things. *Security and Communication Networks*.

Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Roberts, H., Taddeo, M., & Floridi, L. (2021). The ethics of algorithms: key problems and solutions. *Ethics, governance, and policies in artificial intelligence.*, 97-123.

Tschantz, M. C., Sen, S., & Datta, A. (2020). SoK: Differential privacy as a causal property. *In 2020 IEEE Symposium on Security and Privacy, IEEE.*, 354-371.

Tukur, Y. M., Thakker, D., & Awan, I. U. (2021). Edge-based blockchain-enabled anomaly detection for insider attack prevention in Internet of Things. *Transactions on Emerging Telecommunications Technologies*, *32*(6), e4158.

Tzanou, M. (2023). Health Data Privacy Under the GDPR. *TAYLOR & FRANCIS Limited.*

Ullah, H. S., Aslam, S., & Arjomand, N. (2020). Blockchain in healthcare and medicine: A contemporary research of applications, challenges, and future perspectives. *arXiv preprint arXiv:2004.*, 06795.

Vanaparthi, R., & Rao, S. V. (2023). REVOLUTIONIZING HEALTH CARE: AI-ENABLED DISEASE DIAGNOSIS, OUTCOME PREDICTION& OPERATIONAL EFFICIENCY. *Turkish Journal of Computer and Mathematics Education (TURCOMAT),, 14*(03), 993-1001.

Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. *Electronics, 13*(16), 3343.

Vardalachakis, M., & Tampouratzis, M. (2024). Privacy Preservation in IoT: Anonymization Methods and Best Practices. *In 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES) IEEE.*, 1 - 6.

Velmovitsky, P. E., Bublitz, F. M., Fadrique, L. X., & Morita, P. P. (2021). Blockchain applications in health care and public health: increased transparency. *JMIR medical informatics., 9*(6), e20713.

Verma, S., K. Y., Fadlullah, Z. M., Nishiyama, H., & Kato, N. (2017). A survey on network methodologies for real-time analytics of massive IoT data and open research issues. *IEEE Communications Surveys & Tutorials., 19*(3), 1457-1477.

Vourganas, I., Attar, H., & Michala, A. L. (2022). Accountable, responsible, transparent artificial intelligence in ambient intelligence systems for healthcare. *In Intelligent healthcare: infrastructure, algorithms and management. Singapore: Springer Nature Singapore.*, 87-111.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 494.

Wang, J., Spicher, N., Warnecke, J. M., Haghi, M., Schwartze, J., & Deserno, T. M. (2021). Unobtrusive health monitoring in private spaces: The smart home. *Sensors., 21*(3), 864.

Wang, Q., Xia, T., Ren, Y., Yuan, L., & Miao, G. (2021). A New Blockchain-Based Multi-Level Location Secure Sharing Scheme. *Applied Sciences, 11*(5), 2260.

Wang, W., Grundy, J., Khalajzadeh, H., Madugalla, A., & Obie, H. O. (2024). Designing Adaptive User Interfaces for mHealth applications targeting chronic disease: A User-Centric. *arXiv preprint arXiv:2405.08302.*

Weichbroth, P. (2025). Usability Issues With Mobile Applications: Insights From Practitioners and Future Research Directions. *arXiv preprint arXiv:2502.05120*.

Wickramasinghe, C. I. (2022). *In International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services. Cham: Springer Nature Switzerland.*, 101-120.

Wickramasinghe, C. I. (2022). *Best-Practice-Based Framework for User-Centric Privacy-Preserving Solutions in Smart Home Environments..In International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services Cham: Springer Nature Switzerland.*, 101-120.

Wickramasinghe, C. I., & Reinhardt, D. (2021). *A user-centric privacy-preserving approach to control data collection, storage, and disclosure in own smart home environments. In International conference on mobile and ubiquitous systems: computing, networking, and services*, 190-206.

Wiertz, S., & Boldt, J. (2022). Evaluating models of consent in changing health research environments. *Medicine, Health Care and Philosophy., 25*(2), 269-280.

Wijayanti, D., Ujianto, E. I., & Rianto, R. (2024). Uncovering Security Vulnerabilities in Electronic Medical Record Systems: A Comprehensive Review of Threats and Recommendations for Enhancement. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)., 10*(1), 73-98.

Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences., 14*(2), 675.

Wirth, C., & Kolain, M. (2018). Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data. *In: W. Prinz & P. Hoschka (Eds.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies*(DOI: http://dx.doi.org/10.18420/blockchain2018_03), ISNN 2510-2591.

Wróbel-Lachowska, M., Dominiak, J., Woźniak, M., Bartłomiejczyk, N., Diethei, D., Wysokińska, A., Romanowski, A. (2023). That's when I put it on': stakeholder perspectives in large-scale remote health monitoring for older adults. *Personal and Ubiquitous Computing., 27*(6), 2193-2210.

Wu, S., Zhang, A., Gao, Y., & Xie, X. (2024). Patient-centric medical service matching with fine-grained access control and dynamic user management. *Computer Standards & Interfaces., 89*, 103833.

Xiao, S., Ye, Y., Kanwal, N., Newe, T., & Lee, B. (2022). SoK: context and risk-aware access control for zero trust systems. *Security and Communication Networks., 1*, 7026779.

Xiao, Y., & Xiong, L. (2015). Protecting locations with differential privacy under temporal correlations. *In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, 1298-1309.

Yan, W., Wang, Z., Wang, H., Wang, W., Li, J., & Gui, X. (2022). Survey on recent smart gateways for smart home: Systems, technologies, and challenges. *Transactions on Emerging Telecommunications Technologies., 33*(6), e4067.

Yánez, W., Mahmud, R., Bahsoon, R., Zhang, Y., & Buyya, R. (2020). Data allocation mechanism for Internet-of-Things systems with blockchain. *IEEE Internet of Things Journal., 7*(4), 3509-3522.

Yao, X., Farha, F., Li, R., Psychoula, I., Chen, L., & Ning, H. (2021). Security and privacy issues of physical objects in the IoT: Challenges and opportunities. *Digital Communications and Networks., 7*(3), 373-384.

Yao, Y. (2019). Designing for better privacy awareness in smart homes. *In Companion Publication of the 2019 Conference on Computer Supported Cooperative Work and Social Computing.*, 98-101.

Yassine, A., Singh, S., Hossain, M. S., & Muhammad, G. (2019). IoT big data analytics for smart homes with fog and cloud computing. *Future Generation Computer Systems., 91*, 563-573.

Yu, L., Liu, L., Pu, C., Gursoy, M. E., & Truex, S. (2019). Differentially private model publishing for deep learning. *In 2019 IEEE symposium on security and privacy (SP) IEEE.*, 332-349.

Yusupova, G., & Ismailov, A. (2023). Advancing Robust and Ethical Data Minimization Techniques: Theoretical Foundations and Practical Implementations. *Journal of Intelligent Connectivity and Emerging Technologies, 8*(2), 35-47.

Yuvaraj, N., Praghash, K., & Karthikeyan, T. (2022). Privacy preservation of the user data and properly balancing between privacy and utility. . *International Journal of Business Intelligence and Data Mining., 20*(4), 394-411.

Zaman, S., Khandaker, M. R., Khan, R. T., Tariq, F., & Wong, K. K. (2022). Thinking out of the blocks: Holochain for distributed security in iot healthcare. *Ieee Access., 10*, 37064-37081.

Zavalyshyn, I., Legay, A., Rath, A., & Rivière, E. (2022). Sok: Privacy-enhancing smart home hubs. *Proceedings on Privacy Enhancing Technologies.*

Zhang, A., & Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems, 42*(8), 140.

Zhang, S., Yang, S., Zhu, G., Luo, E., Zhang, J., & Xiang, D. (2021). A fine-grained access control scheme for electronic health records based on roles and attributes. *In International Conference on Ubiquitous Security. Singapore: Springer Singapore.*, 25-37.

Zhang, W., Shanmugam, S., & Allen, J. G. (2023). Comparing Smart City Data Protection Approaches: Digital Consent and the Accountability Framework in Singapore. *SMU Centre for AI & Data Governance Research Paper.*, 2.

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the Internet of Things. *IEEE Internet of Things Journal., 6*(2), 1594-1605.

Zheng, X., Mukkamala, R. R., Vatrapu, R., & Ordieres-Mere, J. (2018). Blockchain-based personal health data sharing system using cloud storage. *In 2018 IEEE 20th international conference on e-health networking, applications and services (Healthcom) IEEE.*, 1 - 6.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems., 105*, 475 - 491.

Zhou, I., Makhdoom, I., Shariati, N., Raza, M.A., Keshavarz, R., Lipman, J., Abolhasan, M. and Jamalipour, A. (2021). Internet of things 2.0: Concepts, applications, and future directions. *IEEE Access, 9*, 70961-71012.

Zhou, L., Diro, A., Saini, A., & Kaisar, S. H. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications, 80,* 103678.

Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. *In 2015 IEEE Security and Privacy Workshops. IEEE.*, 180-184.

Appendices

Appendix A: Core Principles of Key Privacy Regulations: GDPR, PIPEDA, HIPAA, and CCPA

Core Principles of Key Privacy Regulations: GDPR, PIPEDA, HIPAA, and CCPA (EUR-Lex, 2016; OPC, 2019; Edemekong et al., 2018; ASPE, 1996; OAG, 2018).

Regulation	Principles	Description
GDPR	Lawfulness, Fairness, and Transparency	Data processing must be lawful, fair, and transparent to individuals.
	Purpose Limitation	Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
	Data Minimization	Data collection should be limited to what is necessary in relation to the purposes for which it is processed.
	Accuracy	Personal data must be accurate and kept up to date.
	Storage Limitation	Personal data must be kept in a form that permits identification of data subjects for no longer than necessary.
	Integrity and Confidentiality	Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing.
	Accountability	The data controller is responsible for, and must be able to demonstrate, compliance with these principles.
PIPEDA	Accountability	Organizations are responsible for personal information under their control and must designate an individual to ensure compliance with the principles.
	Identifying Purposes	Organizations must identify the purposes for collecting personal information at or before the time of collection.
	Consent	Knowledge and consent of the individual are required for the collection, use, or disclosure of personal information.
	Limiting Collection	The collection of personal information must be limited to what is necessary for the identified purposes.
	Limiting Use, Disclosure, and Retention	Personal information must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. It must be retained only as long as necessary to fulfil those purposes.
	Accuracy	Personal information must be accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
	Safeguards	Personal information must be protected by security safeguards appropriate to the sensitivity of the information.
	Openness	An organization must make information about its policies and practices relating to the management of personal information readily available to individuals.
	Individual Access	Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and must be given access to that information.
	Challenging Compliance	An individual can challenge an organization's compliance with the above principles through the individual accountable for the organization's compliance.
HIPAA	Privacy Rule	Protects the privacy of individually identifiable health information (PHI) and sets limits on the use and disclosure of such information without patient authorization.
	Security Rule	Requires covered entities to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI (ePHI).
	Breach Notification Rule	Requires covered entities to notify affected individuals, the Secretary of HHS, and, in some cases, the media, of a breach of unsecured PHI.
	Enforcement Rule	Establishes procedures for investigations and penalties for non-compliance with HIPAA standards.
	Minimum Necessary Rule	Requires that only the minimum necessary information be used, disclosed, or requested to accomplish the intended purpose.
CCPA	Right to Know	Provides consumers the right to request deletion of personal information held by a business, subject to certain exceptions.
	Right to Delete	Provides consumers the right to request deletion of personal information held by a business, subject to certain exceptions.
	Right to Opt-Out	Grants consumers the ability to opt-out of the sale of their personal information to third parties.
	Non-Discrimination	Prohibits businesses from discriminating against consumers who exercise their rights under the CCPA.
	Data Security Provisions	Requires businesses to implement and maintain reasonable security procedures to protect consumers' personal information.

Appendix B: Artefacts in Chapter 4 - Design and Architecture

Appendix B: Artefacts in Chapter 4 - Design and Architecture

All code snippets in this appendix, along with their complete implementations, are available in the GitHub repository. The repository provides additional context and serves as a comprehensive resource for reviewing the implementation details.

a) Code Snippets in Chapter 4

All code snippets in this appendix, along with their complete implementations, are available in the GitHub repository. The repository provides additional context and serves as a comprehensive resource for reviewing the implementation details.

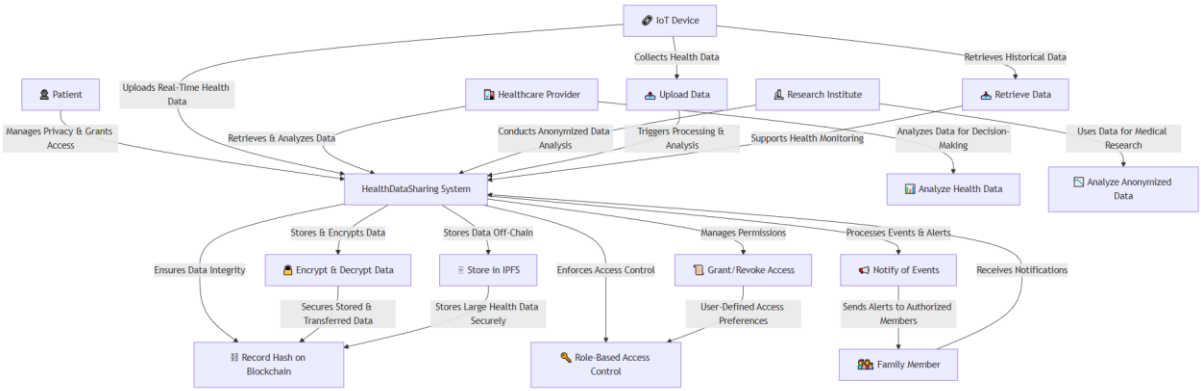


Figure 4.2(b): Detailed UCD of the Proposed HealthDataSharing System in the Ethereum Blockchain Network Environment

B1:Snippet 4.1: Privacy Score Access Control Functions

```Solidity
// Privacy score management with access control
function checkAccessPermission(address requester) public view returns (bool) {
    require(patientPrivacyScore[msg.sender] > 0, "Privacy score not set");
    uint8 score = patientPrivacyScore[msg.sender];
    return validateAccess(requester, score);
}

// Data access with privacy validation
function getData(address patient) public view returns (string memory) {
    require(checkAccessPermission(msg.sender), "Access denied based on privacy score");
    return retrieveData(patient);
}
```

Note: The complete implementation is accessible in the GitHub repository.

B2: Consent Management for Research Institute Data Access

Algorithm 1 Consent Management for Research Institute Data Access

Require: Patient address *patient*, Research Institute address *researchInstitute*, Health data *data*
Ensure: Secure health data sharing based on patient consent

1: **function** SETCONSENTTORI(consent)
2: **Require:** *onlyRegisteredPatient*
3: $patientConsentToRI[msg.sender] \leftarrow consent$
4: **Emit** PatientConsentToRI($msg.sender, consent$)
5: **end function**
6: **function** SENDHEALTHDATATORI(patient, researchInstitute, data)
7: **Require:** *onlyRegisteredExpert*
8: **if** $\neg patientConsentToRI[patient]$ **then**
9: **Throw:** "Patient has not given consent to share data with R.I."
10: **end if**
11: **if** $\neg patientExperts[patient][msg.sender]$ **then**
12: **Throw:** "Not authorised to send data for this patient"
13: **end if**
14: **if** $\neg researchInstitutes[researchInstitute].isRegistered$ **then**
15: **Throw:** "Research institute not registered"
16: **end if**
17: **Emit** HealthDataSentToRI($msg.sender, patient, researchInstitute, data$)
18: NOTIFYFAMILYMEMBERS(patient, "Health data sent to Research Institute")
19: **end function**

Note: The complete code-design is available in the GitHub repository.

B3: Enhanced MDDC Structures

```Solidity
contract MDCCConsentManager {
  // Existing consent tracking
  mapping(address => bool) public patientConsentToRI;

  // Enhanced MDCC structures
  struct DataSensitivity {
    uint8 environmentalData; // Base: 30%
    uint8 wellbeingActivity; // Base: 60%
    uint8 medicalRecords;    // Base: 90%
    uint8 contextMultiplier; // Dynamic: 0-100%
  }

  struct RoleWeight {
    uint8 healthcareProvider; // Base: 90%
    uint8 familyMember;       // Base: 70%
    uint8 researcher;         // Base: 50%
    bool isActive;
  }

  struct TimeDecay {
    uint256 timestamp;
    uint256 expiryPeriod;     // Configurable expiry
    uint8 decayRate;          // Per time unit
```

```
    }

    struct ConsentContext {
        DataSensitivity sensitivity;
        RoleWeight roleWeight;
        TimeDecay timeDecay;
        bool isEmergency;
        uint256 lastUpdated;
    }
}
```

Note: The complete implementation and its role within the MDDC functionality are accessible in the GitHub repository.

B4: Enhanced MDDC Mappings and Events

```Solidity
// Enhanced mappings
mapping(address => ConsentContext) public patientConsent;
mapping(address => mapping(address => bool)) public patientExpertConsent;

// Events for transparency
event ConsentUpdated(
    address indexed patient,
    address indexed requester,
    uint256 sensitivityScore,
    uint256 roleWeight,
    uint256 timestamp
);

event EmergencyAccessGranted(
    address indexed patient,
    address indexed provider,
    uint256 timestamp
);
```

Note: The complete implementation, including its integration into the MDDC system, is available in the GitHub repository.

B5(i): Core MDDC Consent Score Computation

```Solidity
// Core MDCC consent computation
function computeConsentScore(
    address patient,
    address requester,
    string memory dataType
) public view returns (uint256) {
    ConsentContext memory context = patientConsent[patient];

    // Base sensitivity score
    uint256 sensitivityScore = getSensitivityScore(context.sensitivity, dataType);

    // Apply role weight
    uint256 roleScore = getRoleWeight(context.roleWeight, requester);
```

```
    // Calculate time decay
    uint256 timeScore = calculateTimeDecay(context.timeDecay);

    // Emergency override check
    if (context.isEmergency && isHealthcareProvider(requester)) {
        return type(uint256).max;
    }

    // Final weighted score
    return (sensitivityScore * roleScore * timeScore) / 10000;
}

// Consent validation with MDCC
function validateConsent(
    address patient,
    address requester,
    string memory dataType
) public view returns (bool) {
    uint256 consentScore = computeConsentScore(patient, requester, dataType);
    uint256 threshold = getConsentThreshold(dataType);

    return consentScore >= threshold;
}
```

Note: The complete implementation and its integration within the MDDC framework are available in the GitHub repository.

B5(ii): Updating Consent with Context

```Solidity
// Update consent with context
function updateConsent(
    address requester,
    string memory dataType,
    bool consent
) public {
    require(msg.sender != address(0), "Invalid patient address");

    ConsentContext storage context = patientConsent[msg.sender];
    context.lastUpdated = block.timestamp;

    if (consent) {
        patientExpertConsent[msg.sender][requester] = true;
    } else {
        patientExpertConsent[msg.sender][requester] = false;
    }

    emit ConsentUpdated(
        msg.sender,
        requester,
        getSensitivityScore(context.sensitivity, dataType),
        getRoleWeight(context.roleWeight, requester),
```

```
        block.timestamp
    );
}

// Emergency access control
function setEmergencyAccess(bool status) public {
    require(msg.sender != address(0), "Invalid patient address");

    ConsentContext storage context = patientConsent[msg.sender];
    context.isEmergency = status;

    if (status) {
        emit EmergencyAccessGranted(
            msg.sender,
            address(0),
            block.timestamp
        );
    }
}
```

Note: The complete implementation is available in the GitHub repository.

B5(iii): MDDC Role Control Contract

```Solidity
contract MDCCRoleControl {
    // Role weights as constants
    uint256 private constant HEALTHCARE_WEIGHT = 90;    // 0.9
    uint256 private constant EMERGENCY_WEIGHT = 95;     // 0.95
    uint256 private constant FAMILY_WEIGHT = 70;        // 0.7
    uint256 private constant RESEARCHER_WEIGHT = 50;    // 0.5

    struct RoleWeight {
        uint256 weight;
        bool isActive;
        bool canAccessMedical;
        bool canAccessLifestyle;
        bool canAccessEnvironmental;
    }

    mapping(address => RoleWeight) public userRoles;
    event RoleAssigned(address user, string role, uint256 weight);

    function assignRole(address user, string memory role) public {
        RoleWeight storage userRole = userRoles[user];

        if (compareStrings(role, "HealthcareProvider")) {
            userRole.weight = HEALTHCARE_WEIGHT;
            userRole.canAccessMedical = true;
        } else if (compareStrings(role, "FamilyMember")) {
            userRole.weight = FAMILY_WEIGHT;
            userRole.canAccessLifestyle = true;
        } else if (compareStrings(role, "Researcher")) {
            userRole.weight = RESEARCHER_WEIGHT;
```

```
            userRole.canAccessEnvironmental = true;
        }
        userRole.isActive = true;
        emit RoleAssigned(user, role, userRole.weight);
    }

    function getRoleWeight(address user) public view returns (uint256) {
        require(userRoles[user].isActive, "User role not active");
        return userRoles[user].weight;
    }
}
```

Note: The complete implementation is available in the GitHub repository.

B5(iv): MDDC Consent Manager Contract

```Solidity
contract MDCCConsentManager {
    struct ConsentSetting {
        bool isValid;
        uint256 validUntil;
        mapping(string => bool) dataTypeConsent;
        mapping(address => bool) approvedRequester;
    }

    mapping(address => ConsentSetting) public patientConsent;
    event ConsentUpdated(
        address indexed patient,
        string dataType,
        bool consent,
        uint256 validUntil
    );

    function updateConsent(
        string memory dataType,
        bool consent,
        uint256 validityPeriod
    ) public {
        ConsentSetting storage setting = patientConsent[msg.sender];
        setting.isValid = true;
        setting.validUntil = block.timestamp + validityPeriod;
        setting.dataTypeConsent[dataType] = consent;

        emit ConsentUpdated(
            msg.sender,
            dataType,
            consent,
            setting.validUntil
        );
    }

    function checkConsent(
        address patient,
```

```
        string memory dataType
    ) public view returns (bool) {
        ConsentSetting storage setting = patientConsent[patient];
        return setting.isValid &&
            block.timestamp <= setting.validUntil &&
            setting.dataTypeConsent[dataType];
    }
}
```

Note: The complete implementation is available in the GitHub repository.

B5(v): MDDC Consent Manager Contract

```Solidity
event DataAccess(
    address indexed requester,
    bytes32 indexed dataHash,
    uint256 timestamp,
    AccessType accessType
);

event PrivacyUpdate(
    address indexed subject,
    uint256 oldScore,
    uint256 newScore,
    uint256 timestamp
);
```

Note: The complete implementation and integration of these events within the MDDC system are available in the GitHub repository.

B6: Performance Metrics Sources

This table summarises the five key sources with their corresponding references.

Source Category	Details	References
Healthcare Industry Standards	HL7 FHIR guidelines for data exchange	Sharma et al., 2023; Vorisek et al., 2022
Data Protection Regulations	GDPR, NHS Digital's DSP Toolkit	Mushak, 2023; Mc Cullagh, 2023; Winau, 2023; Murray et al., 2022; Ndumbe & Velikov, 2024; Rotim & Landeka, 2024; Wanecki et al., 2023
HIPAA Technical Safeguards	HIPAA Security Rule requirements	Choi & Williams, 2022; Wells, 2022
Industry Benchmarks for Blockchain Healthcare	MedRec and Healthcare Data Gateway	Azbeg et al., 2022; Singh & Haroon, 2024
International Technical Standards	ISO/IEEE 11073 for healthcare communication, IEC 62304 for software	Adamson, 2023; Granlund et al., 2024

Appendix C: Artefacts in Chapter 5 – Implementation and System Integration

Appendix C: **Artefacts in Chapter 5 – Implementation and System Integration**

a) Code Snippets: GitHub repository.

b) Algorithms:

Algorithm: Web3.js Integration in React Component

This algorithm outlines the procedures for integrating Web3.js into the React-based frontend, enabling secure interactions with the Ethereum blockchain. It handles key functionalities, including:

- Connecting to the Ethereum network.
- Authenticating user accounts via MetaMask.
- Calling smart contract functions for managing consent parameters.
- Listening to blockchain events.

a) Logical Implementation Algorithm

Algorithm 1 Web3.js Integration in React Component

Require: contractABI, contractAddress
Ensure: Initialized Web3 instance, contract instance, and user account

```
procedure InitializeWeb3AndContract
    if window.ethereum exists then
        Request user accounts from MetaMask
        Create new Web3 instance using window.ethereum
        Get user accounts
        Set current account to first account
        Create new contract instance using contractABI and contractAddress
        Set Web3 and contract instances in component state
    else
        Alert user to install MetaMask
    end if
end procedure
procedure HandleAccountsChanged(accounts)
    Set current account to accounts[0]
end procedure
procedure HandleChainChanged
    Reload the page
end procedure
procedure RegisterAsPatient
    if contract instance exists then
        Call registerAsPatient method on contract
        if transaction successful then
            Alert success message
        else
            Alert failure message
        end if
    end if
end procedure
On component mount:
Call InitializeWeb3AndContract()
Set up event listeners for accountsChanged and chainChanged
On component render:
Display current account address
Provide button to call RegisterAsPatient()
```

b) Physical Implementation Algorithm

Algorithm 2 Web3.js Integration in React Component

Require: User consent parameters (e.g., time, purpose, sensitivity)
Ensure: Transaction result reflecting consent updates on the blockchain
Step 1: Establish connection to Ethereum via Web3.js
    a. Detect if MetaMask is installed.
    b. Request user permission to connect their wallet.
    c. Initialize Web3 instance with the provider from MetaMask.
Step 2: Load smart contract
    a. Fetch contract ABI (Application Binary Interface) and address.
    b. Instantiate the contract object using Web3.js.
Step 3: Authenticate user
    a. Retrieve user accounts from MetaMask.
    b. Ensure the selected account matches the smart contract permissions.
Step 4: Submit consent parameters
    a. Call the appropriate smart contract function (e.g., setConsent).
    b. Pass the user-defined consent parameters as input.
    c. Await transaction confirmation from the blockchain.
Step 5: Monitor events
    a. Subscribe to blockchain events emitted by the smart contract.
    b. Log event details for debugging and validation.

Key Algorithms Driving the Process

Implemented series of algorithms (1-6), each focusing on a specific aspect of the data-sharing process that ensures secure, transparent, and patient-controlled sharing of health data between patients and healthcare providers, maintaining the integrity of the data and the privacy preferences of the patient throughout the process.

Algorithm 1 Patient Data Upload and Encryption

Require: Patient health data
Ensure: Encrypted data stored in IPFS, IPFS hash
Read patient health data
Apply encryption (ECC-256r1/AES-128/EAX)
Store encrypted data in IPFS
Receive IPFS hash
Create block in Blockchain with IPFS hash

Algorithm 2 Healthcare Provider Access Request

Require: Provider ID, Patient ID, Purpose of access
Ensure: Access request logged
Initialization:
Verify provider's credentials
if authorised provider **then**
    Create access request with Provider ID, Patient ID, Purpose
    Log request in smart contract
    Notify patient of pending request
end if

Algorithm 3 Patient Consent Management

Require: Access request details
Ensure: Updated access permissions
Initialization: Retrieve access request details
Present request to patient
if patient grants permission **then**
    Update smart contract with approved access
else
    Log denied request
end if

Algorithm 4 ensures that approved stakeholders can securely retrieve encrypted data from IPFS using the CID, decrypt it with appropriate keys, and log access events on the blockchain. Algorithm 5 monitors patient access logs to detect changes in consent settings and dynamically updates access permissions within the smart contract to ensure ongoing compliance. Algorithm 6 enables healthcare providers to analyse decrypted health data, generate

treatment plans or prescriptions, and log data utilisation events on the blockchain to ensure accountability and transparency.

Algorithm 4 Data Retrieval and Decryption

Require: Approved access request, IPFS hash
Ensure: Decrypted health data
1: **Initialization:** Verify provider's permissions in smart contract
2: **if** permissions valid **then**
3: Retrieve encrypted data from IPFS using hash
4: Decrypt data using appropriate keys
5: Log data access event in blockchain
6: **end if**

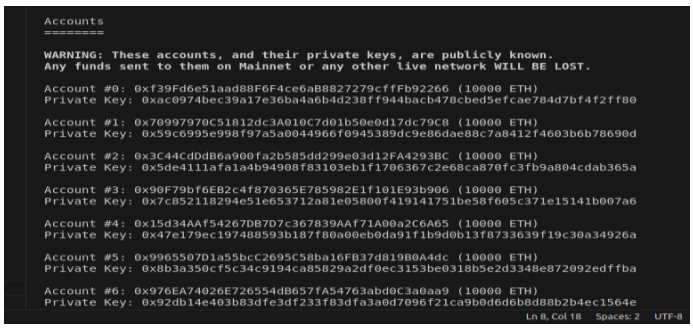
Algorithm 5 Continuous Monitoring and Control

Require: Access logs, Patient preferences
Ensure: Updated access controls
1: **Initialization:** Continuously monitor access logs
2: **if** patient modifies permissions **then**
3: Update smart contract with new permissions
4: Apply new permissions to all future access attempts
5: **end if**

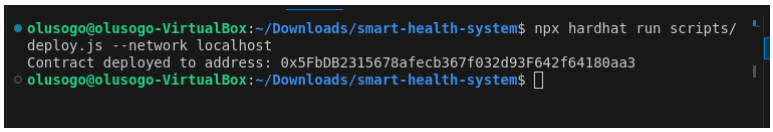
Algorithm 6 Data Utilisation by Healthcare Provider

Require: Decrypted health data
Ensure: Treatment plans, prescriptions
1: **Initialization:** Analyze decrypted health data
2: Generate treatment plans or prescriptions
3: Log data utilization in blockchain

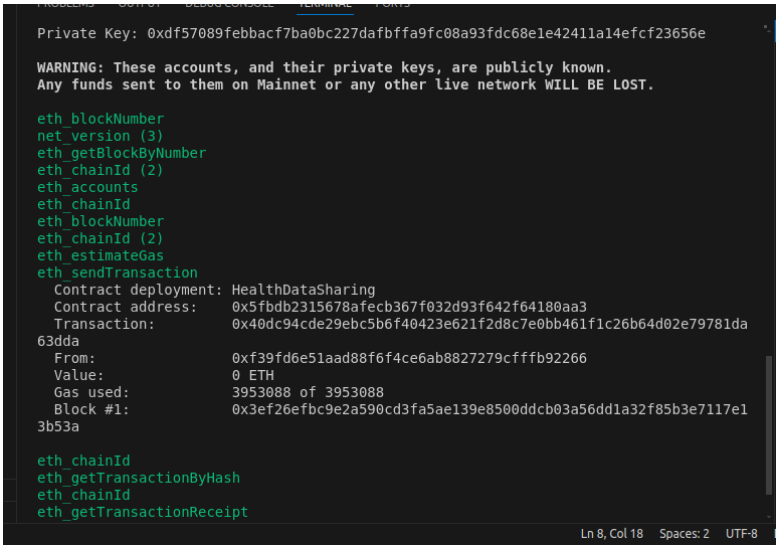
c) Figures:



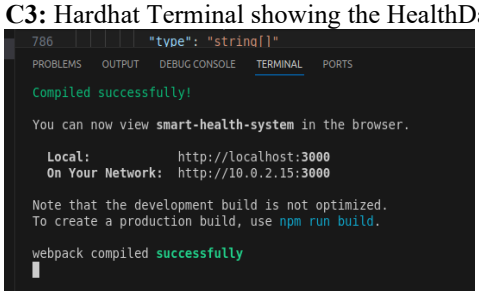
C1: Hardhat Terminal showing the Deployment Of Smart Contract for 20 base accounts



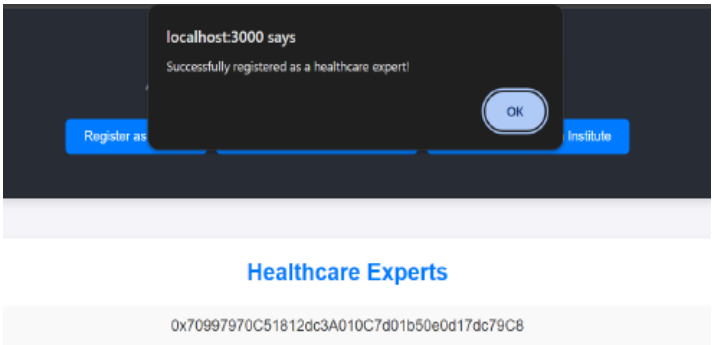
C2: Deployment of Contract to Address



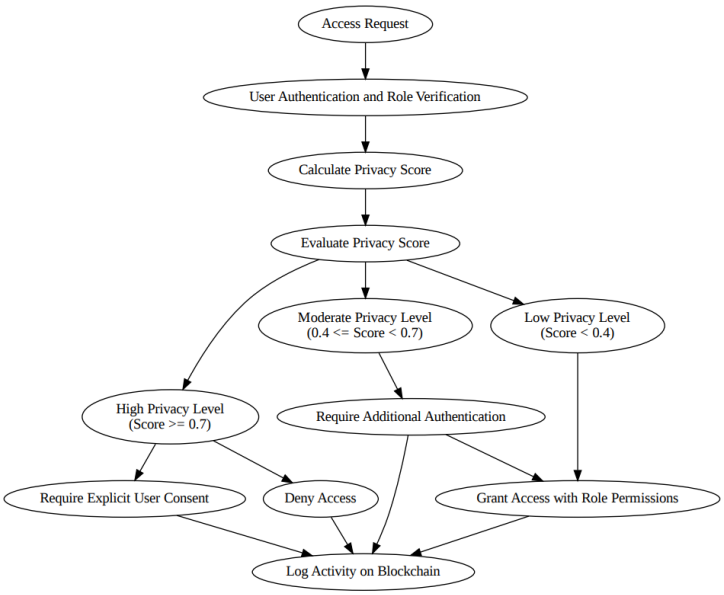
C3: Hardhat Terminal showing the HealthDataSharing Contract Address and 1st Block Log Record



C4: Initiation of React Frontend



C5: Healthcare Expert Registration with Address

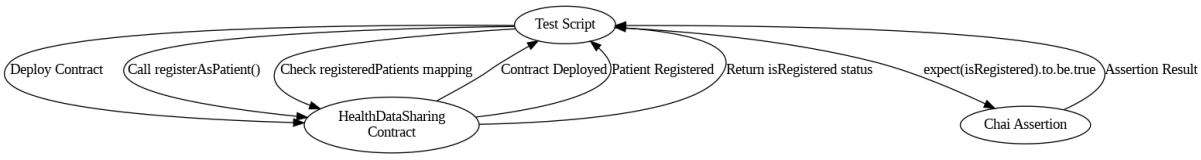


C6(i): Lifecycle of Key Smart Contract Functions in the Privacy Management System

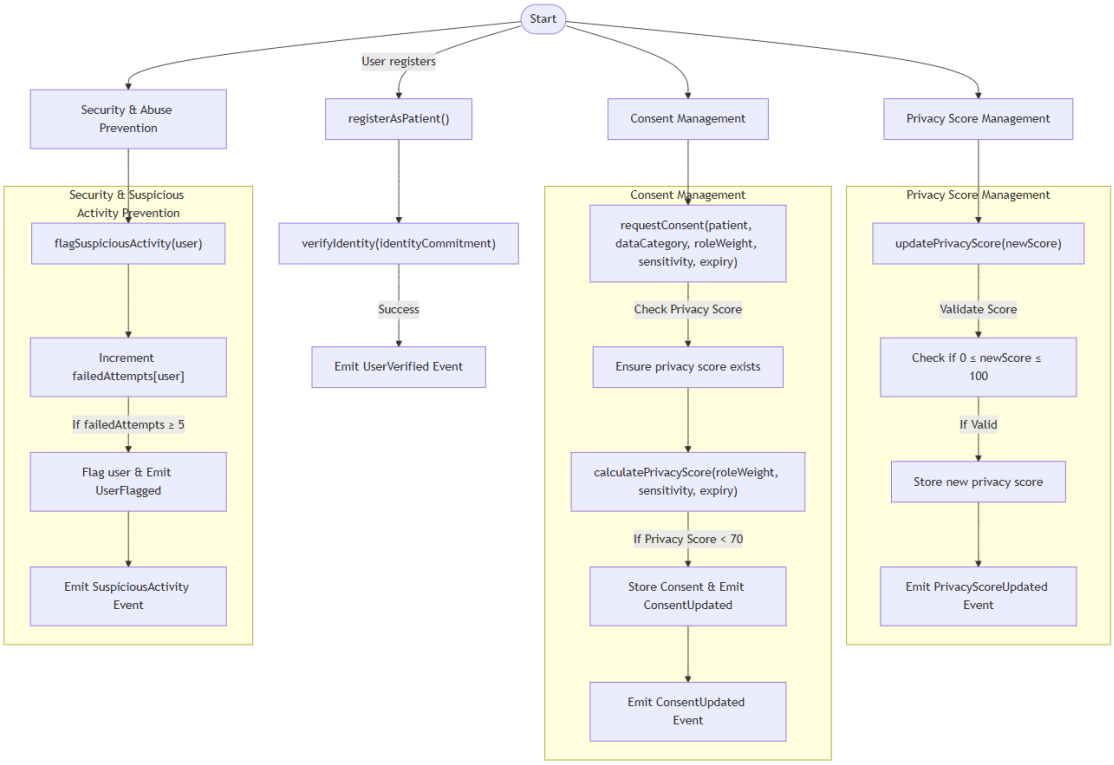
Chai assertions was used for smart contract testing to verify expected behaviors and outcomes. They provide a natural language syntax for writing test conditions, making tests more readable and maintainable, allowing for:

1. Verify transaction results (success/failure)
2. Check event emissions with correct parameters
3. Validate state changes after function calls
4. Test access control mechanisms and permissions
5. Confirm mathematical calculations behave correctly
6. Verify conditional logic executes as expected

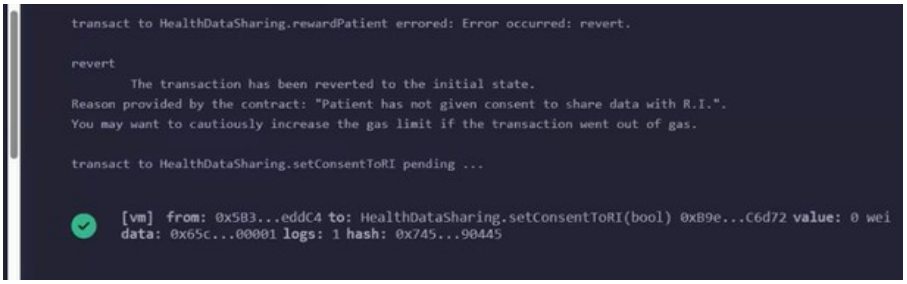
It was used in this privacy-aware framework study to test that consent records are properly stored, access rules are enforced, and privacy scores are calculated accurately by the smart contracts.



C6(ii): Flow Representation of Chai Assertion.



C6(ii): Process Flow of the HealthDataSharing Smart Contract: Registration, Privacy Management, Consent Control, and Security Enforcement.

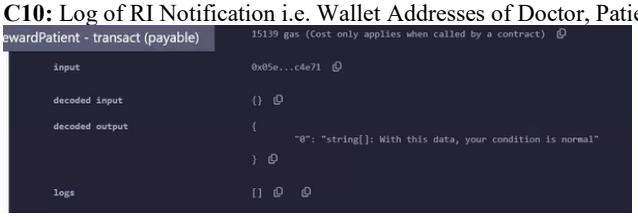


C7: SetConsentToRI Function

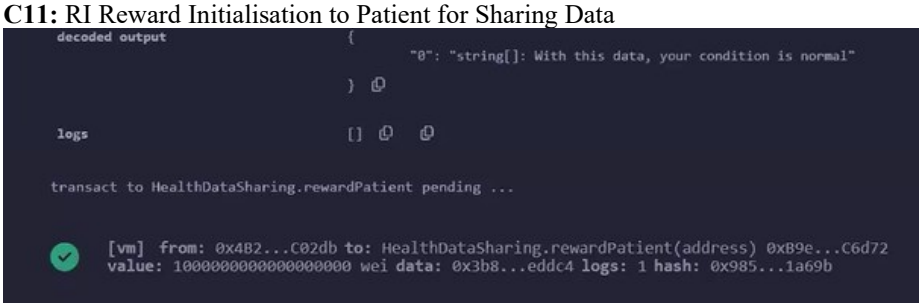
C8: Consent for Healthcare Expert (Doctor) to send data to Research Institute (RI)

C9: The Healthcare Expert (Doctor) Sends Consented Patient Data To RI

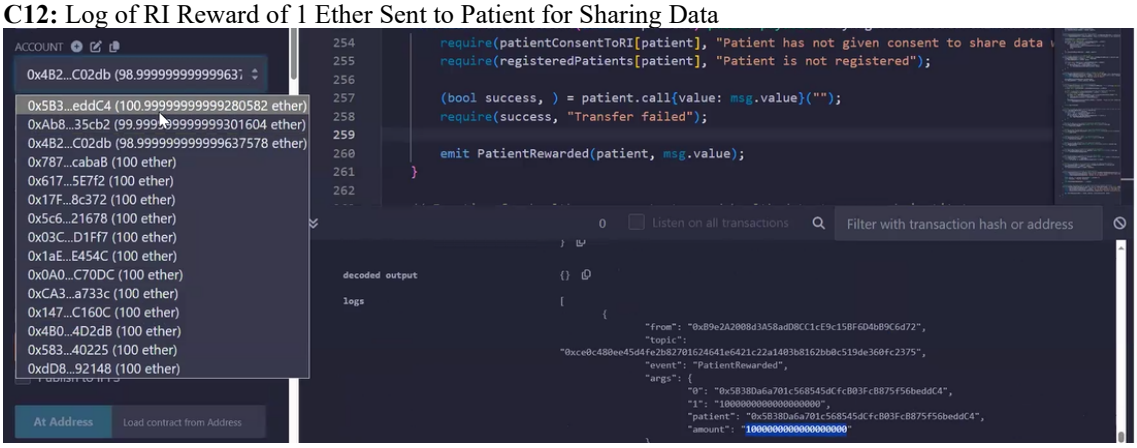
C10: Log of RI Notification i.e. Wallet Addresses of Doctor, Patient, RI, and the CID of Data to be Decrypted



C11: RI Reward Initialisation to Patient for Sharing Data

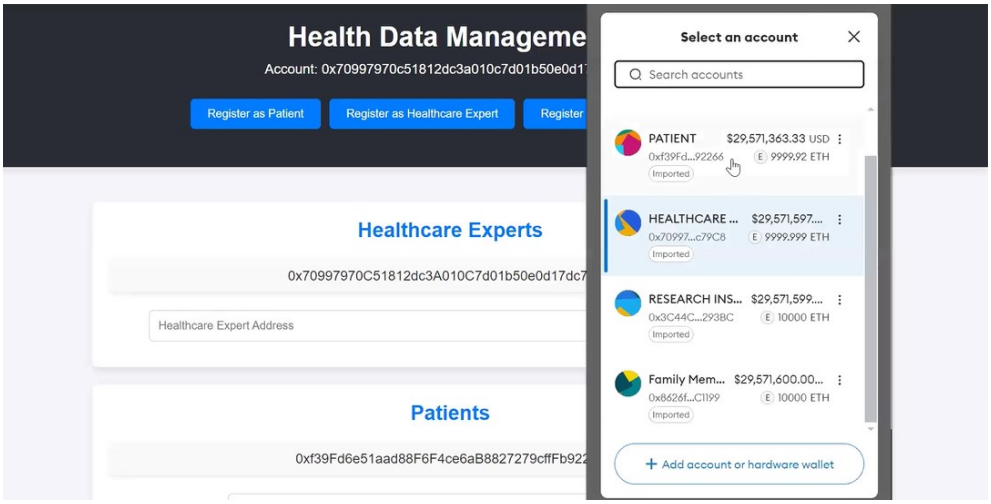


C12: Log of RI Reward of 1 Ether Sent to Patient for Sharing Data

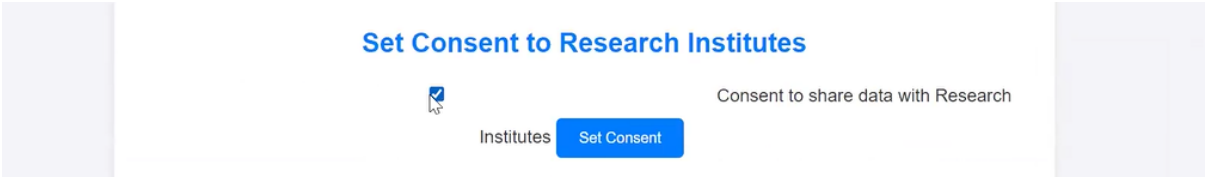


C13: Confirmation of Patient Reward of 1 Ether for Sharing Data

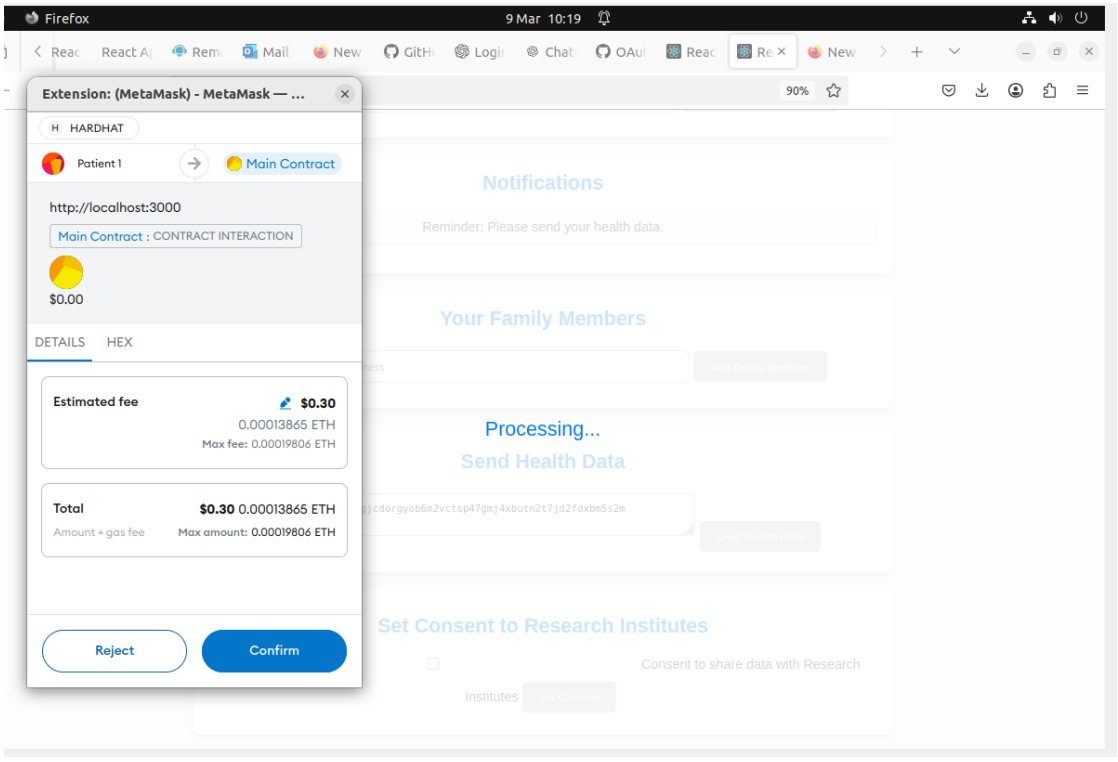
1 Ether = 1 x 10^{18} , as it can be observed, the Patient wallet address (1st) has its Ether increase by 1 Ether while the RI wallet (3rd), has theirs decrease by 1 Ether.



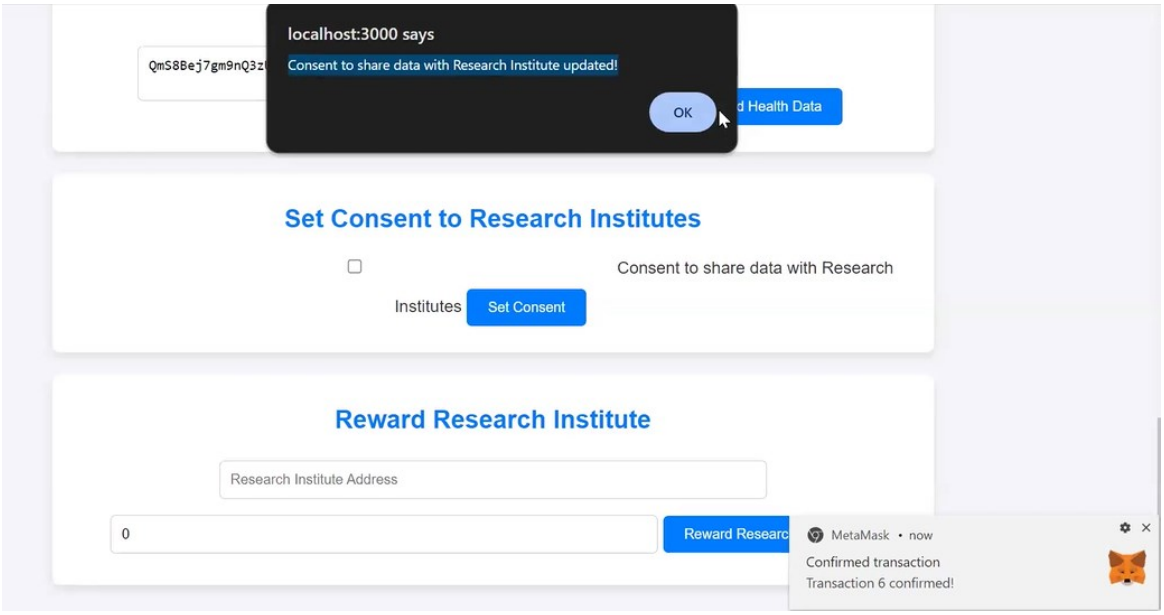
C14: Using HEN Patient authorises and signs the consent permission process (enabling the setConsentToRI) through MetaMask.



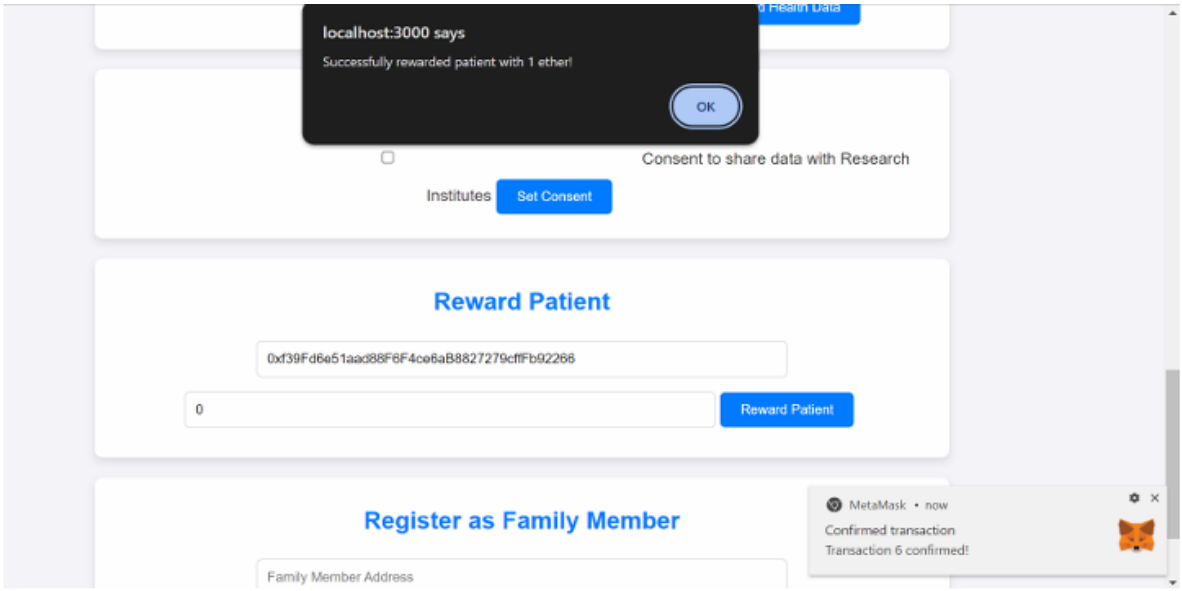
C15: Patient Consent Check-on



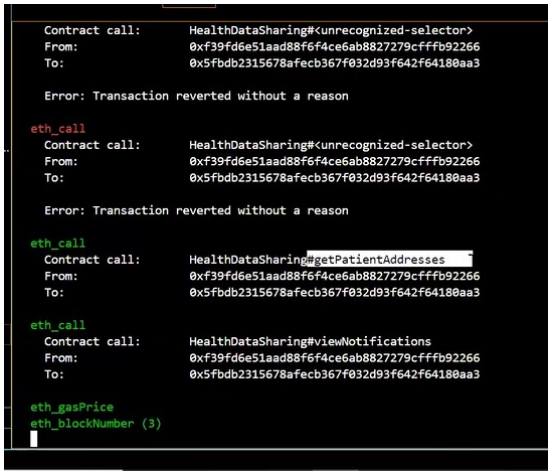
C15: Consent Sign-On Using the Private Key of Patient Address



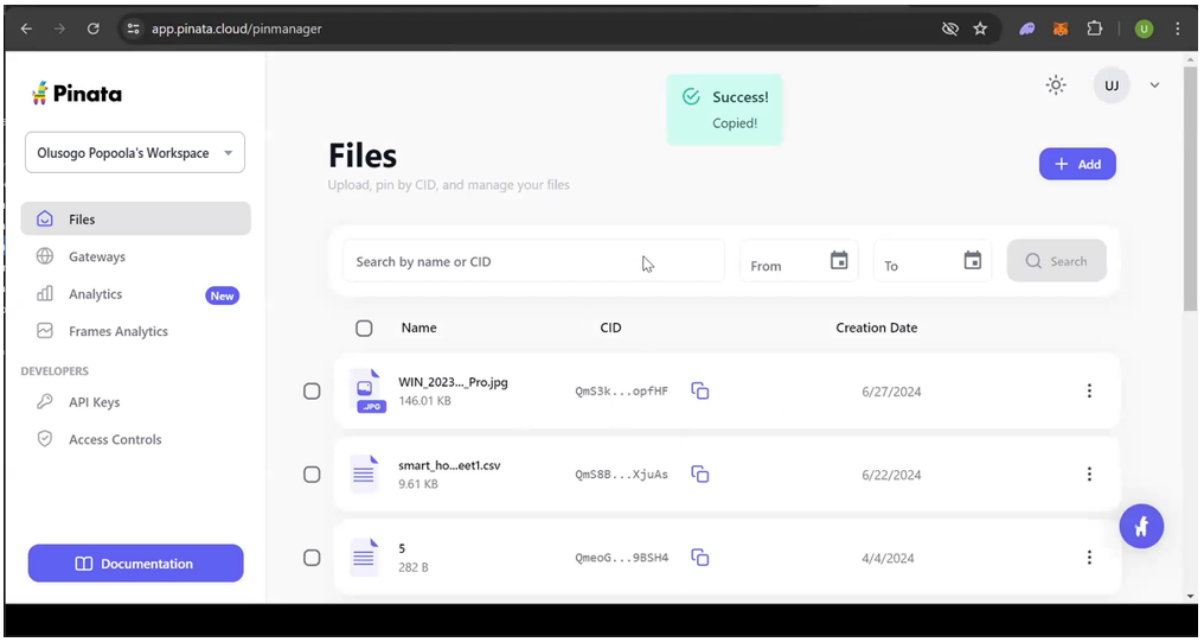
C16: Confirmation of Consent to Share Data Setup



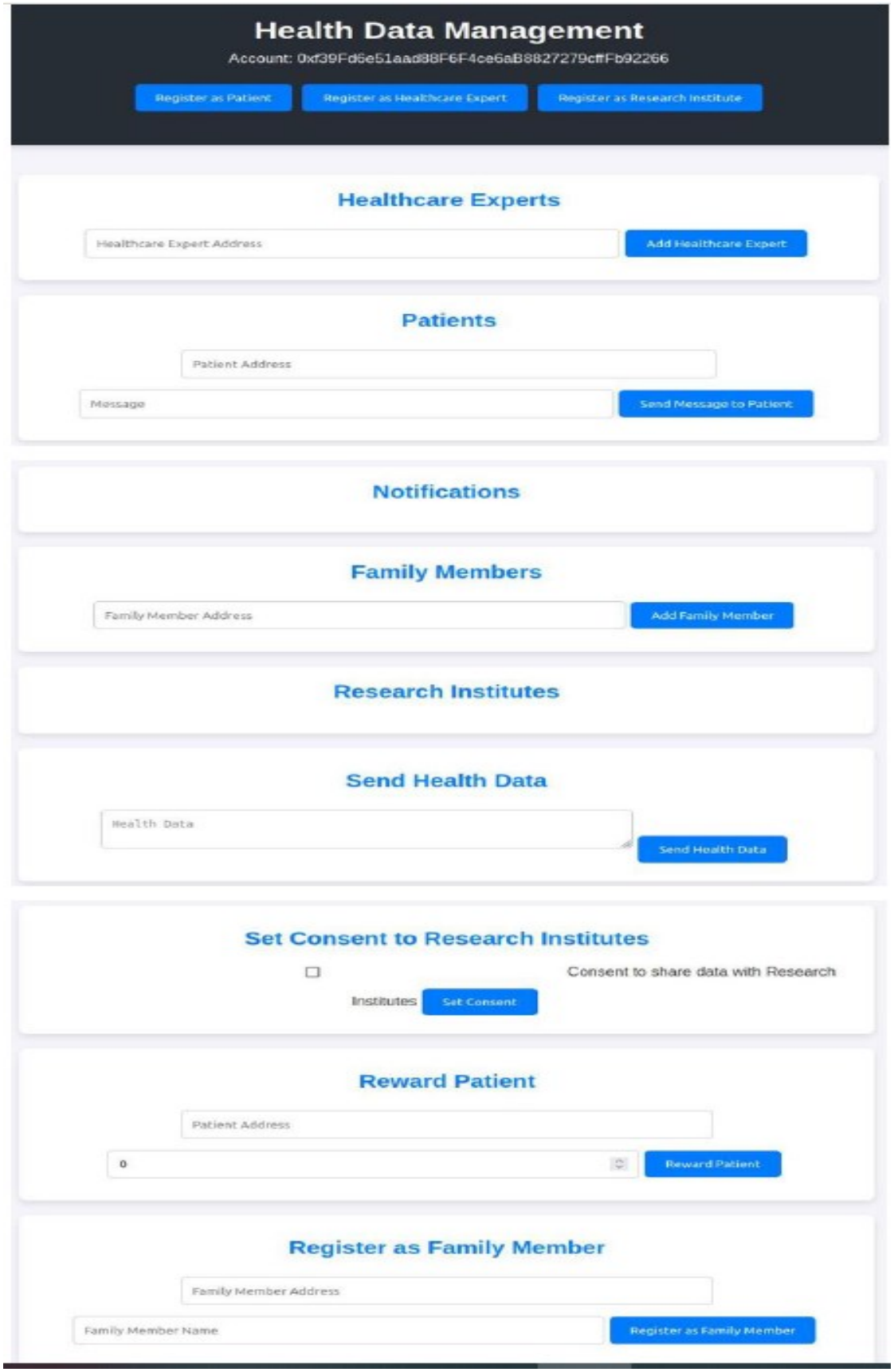
C17: Confirmation of Patient Reward of 1 Ether for Sharing Data on Intuitive React Frontend



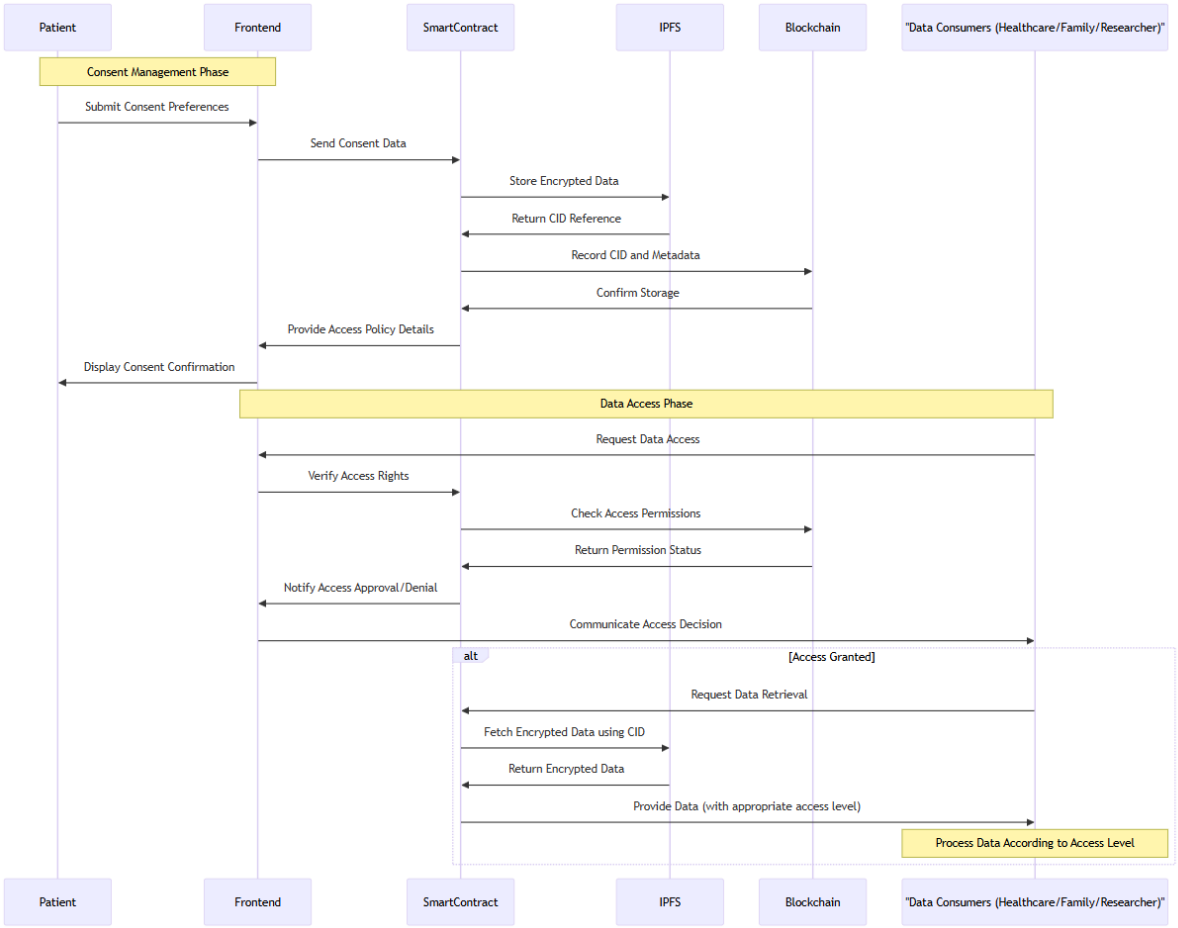
C18: Log Confirming the Successful Communication between the Frontend and the Blockchain



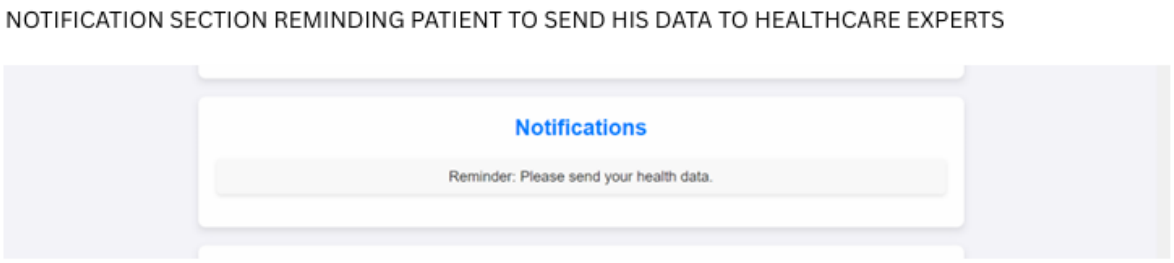
C19: Pinata Gateway IPFS Web Interface



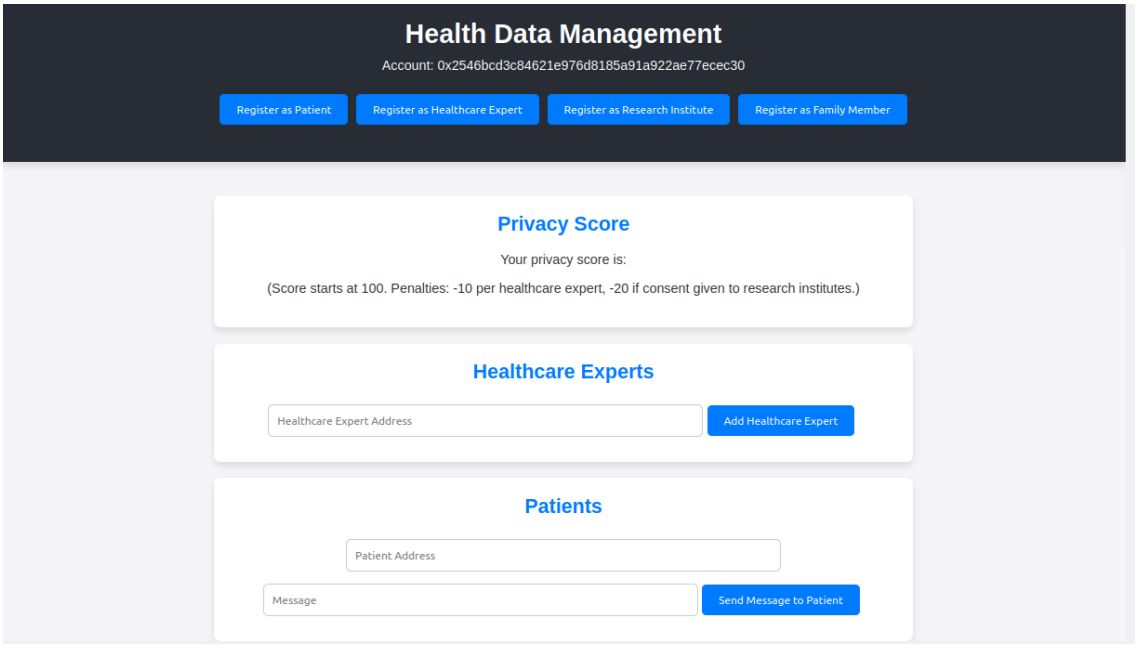
C20: The main dashboard of the *HealthDataSharing* application system



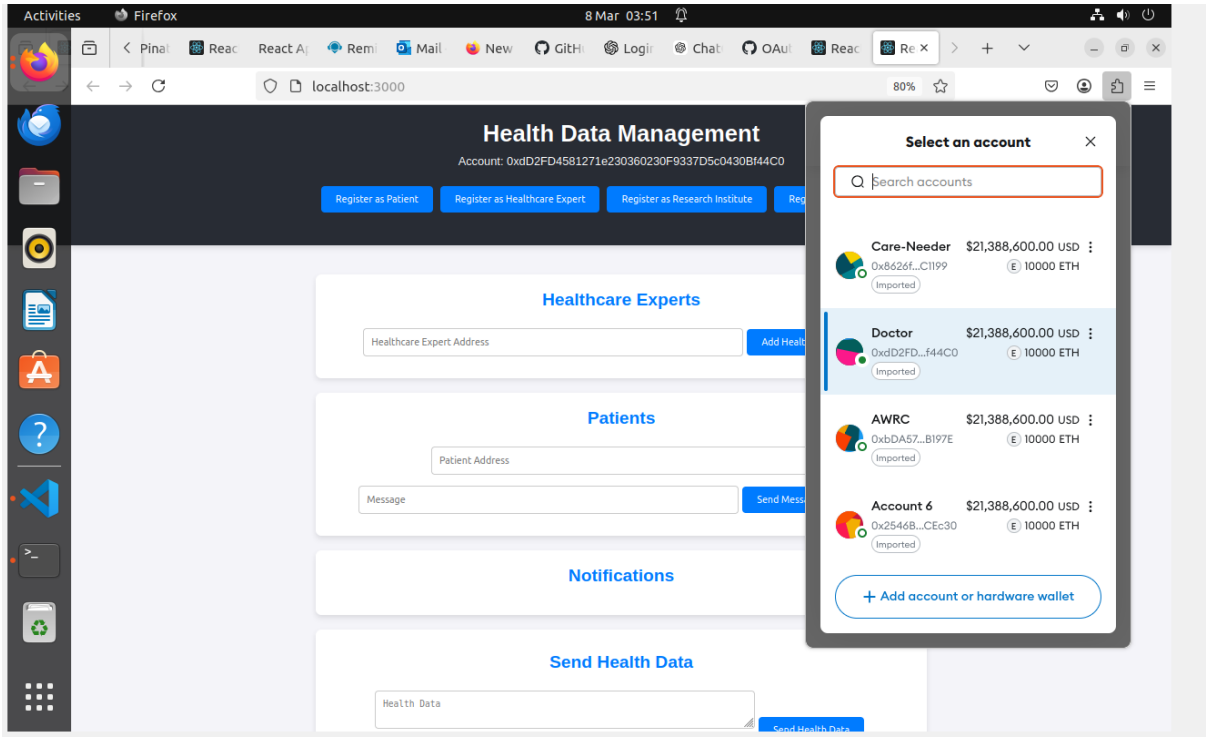
C21: Data Sharing Workflow Interaction



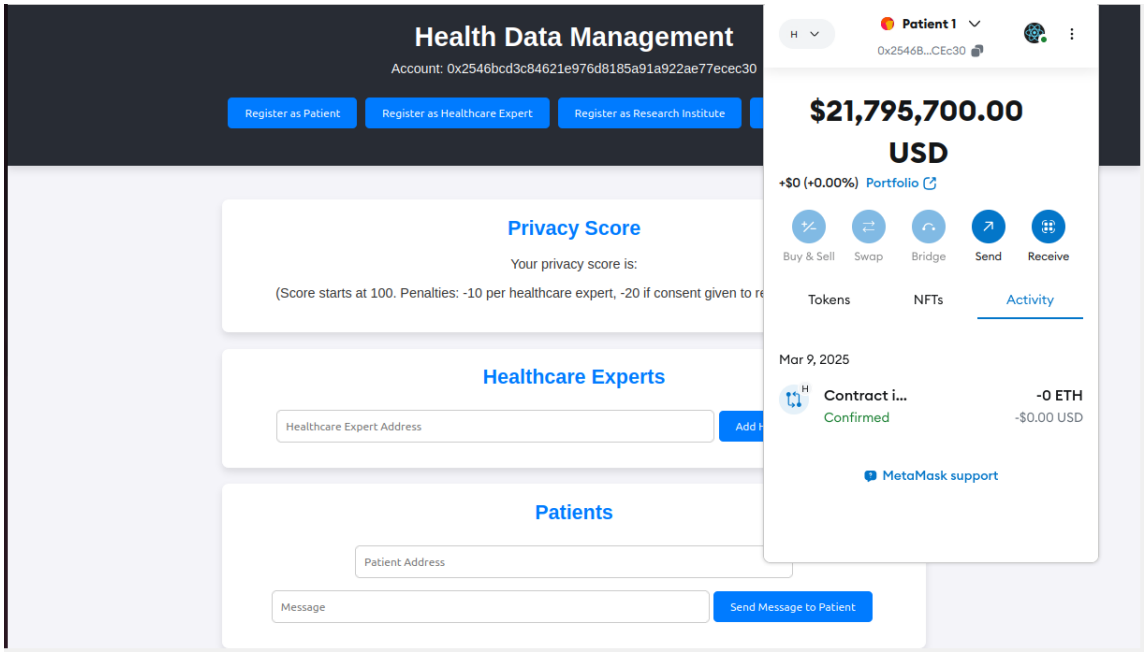
C22: Patient-Centric Data Management and Communication Interface - Notification Prompter



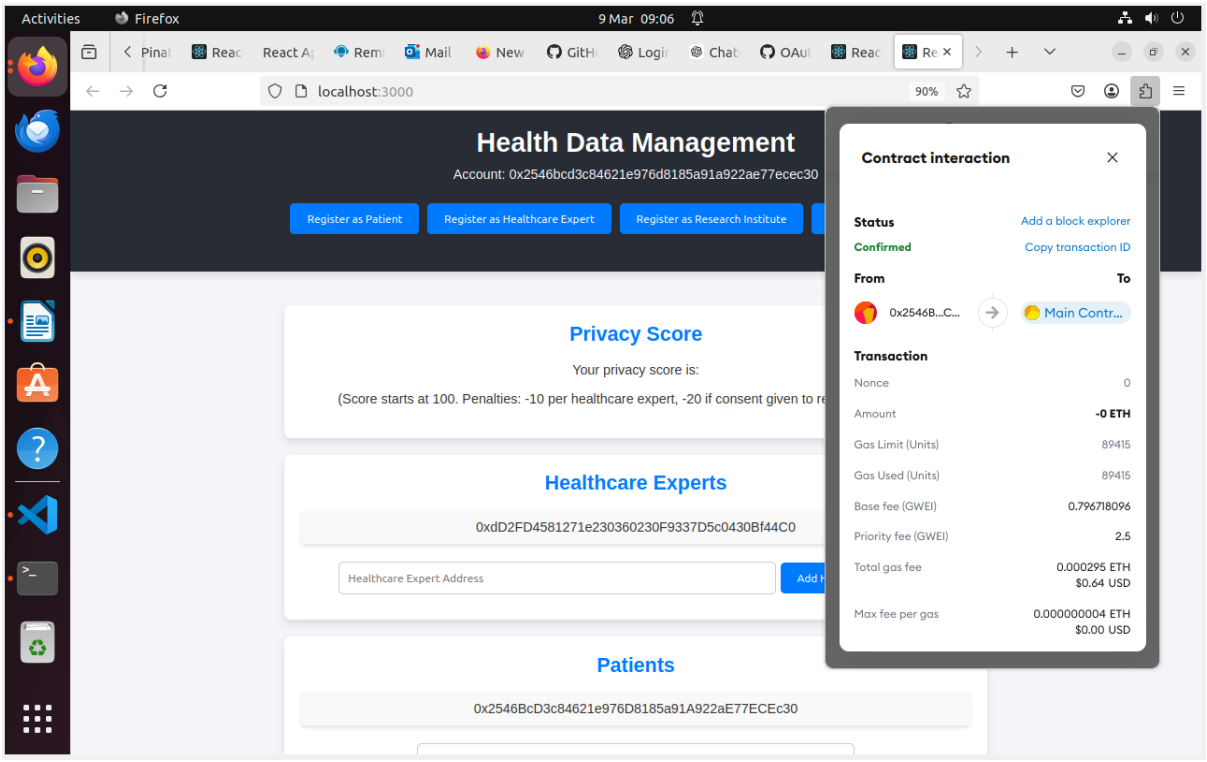
C23(a): The main dashboard of the *HealthDataSharing* application system prior to interatation



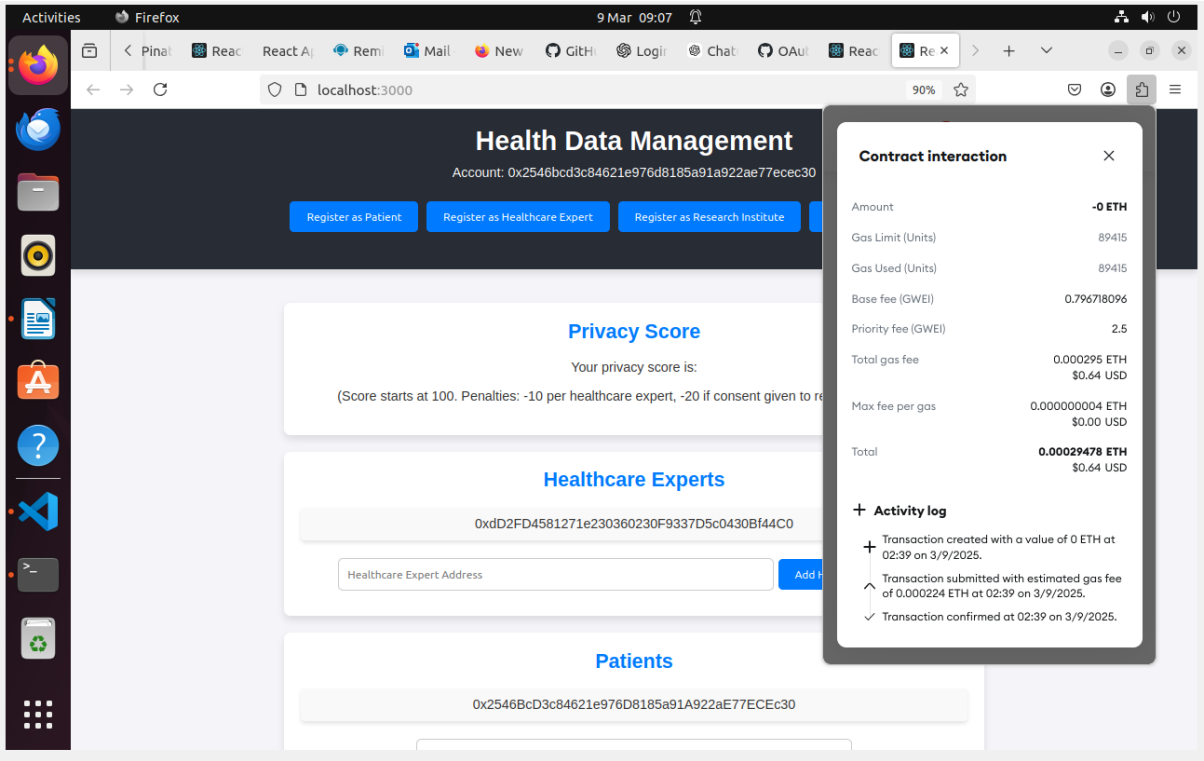
C23(b): The main dashboard of the *HealthDataSharing* application system on tesbed interface with authenticated interaction



C23(c): Confirmation of Gas Fee Usage for Transaction



C23(d): Confirmation of Gas Utilsation per Transaction



C23(d2): Confirmation of Gas Utilsation per Transaction

d) Smart Home Healthcare Testbed Dataset

e) Detailed Section 5.3 here

f) Alternative Details of Data Processing and Model Considerations here

Appendix D: Artefacts in Chapter 6 – Testing, Validation, and User Evaluation

Appendix D: Artefacts in Chapter 6 – Testing, Validation, and User Evaluation

D1: Testing Environment Configuration and Methodology (Section 6.1.1):

Figure D1(a): Server and Network Setup

HTTPS was configured using a Nginx reverse proxy with a self-signed TLS 1.3 certificate to secure communication between the smartwatch and the Raspberry Pi 4 home gateway (for testing/research environments). The smartwatch app authenticated the gateway using the certificate's public key, ensuring encrypted data transmission. In production environments, a publicly trusted certificate, such as one issued by Let's Encrypt, can replace the self-signed certificate to improve compatibility and automate certificate management(for real-world deployment).

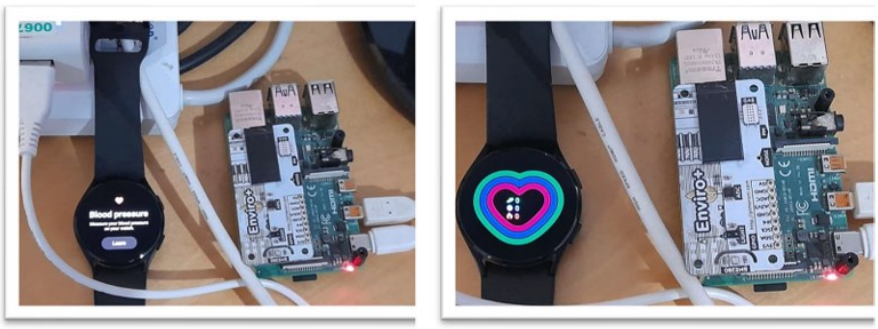


Figure D1(b): IoT Client Setup

Smart Home Healthcare Testbed **Dataset**

D2: Results and Analysis (Section 6.1.2)

i) Near-linear Performance Of Scalability Testing

Figure D2 describes the scalability performance showing (a) response time variation with increasing concurrent requests and (b) system throughput scaling, demonstrating sustained performance up to 15,000 concurrent requests.

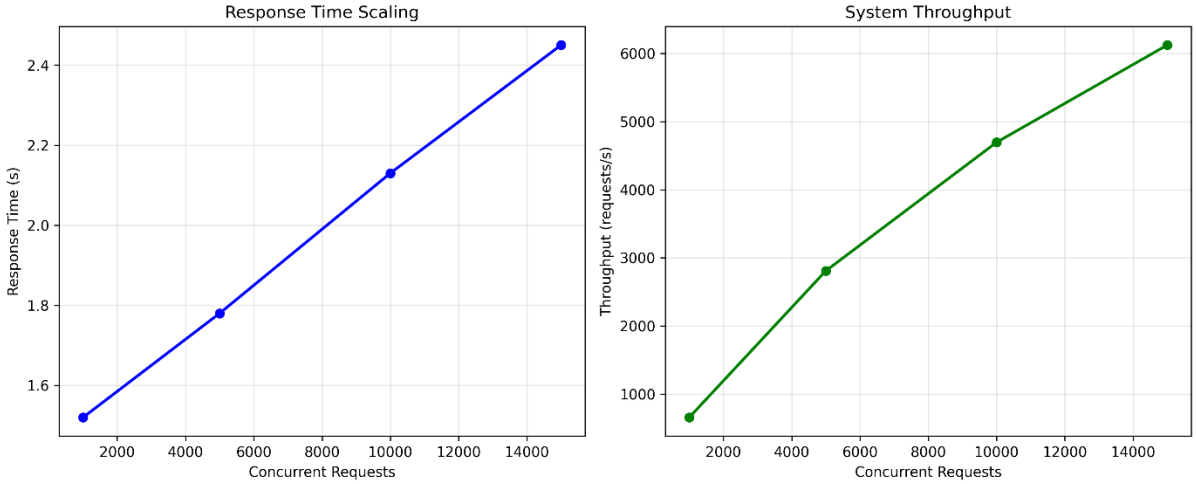


Figure D2(i) : Scalability Analysis showing throughput vs concurrent requests

Log of transactions confirming scalability and stress testing available here

ii) Gas Optimisation and Cost Efficiency

Figure D2(ii) illustrates gas cost trends across various transactions. The *Cumulative Gas Costs Over Time plot* (Figure 6.2(a)) captures a representative 9-minute window, generalising transaction patterns over the full 90-day period. The cumulative gas costs over 9 minutes from deployment to user interactions steadily increased, reaching a total of 106,447.116020388 gwei (0.000106447116020388 ETH), reflects the comprehensive nature of the testing scenario, including smart contract deployment, user registrations, and various system interactions.

Gas Costs per Operation (Figure 6.2(b)) supports Table 6.2, detailing cost variations across transaction types - reveals that deployment operations consumed the highest gas, followed by data upload and user registration. *Gas Cost Distribution* (Figure 6.2(c)) highlights transaction cost efficiency trends - shows the gas cost distribution centered around the average transaction cost of 181,282 gwei (0.000181 ETH), while *Gas Cost vs. Transaction Volume* (Figure 6.2(d)) confirms that cost efficiency remains stable under increasing transaction loads, reinforcing system scalability

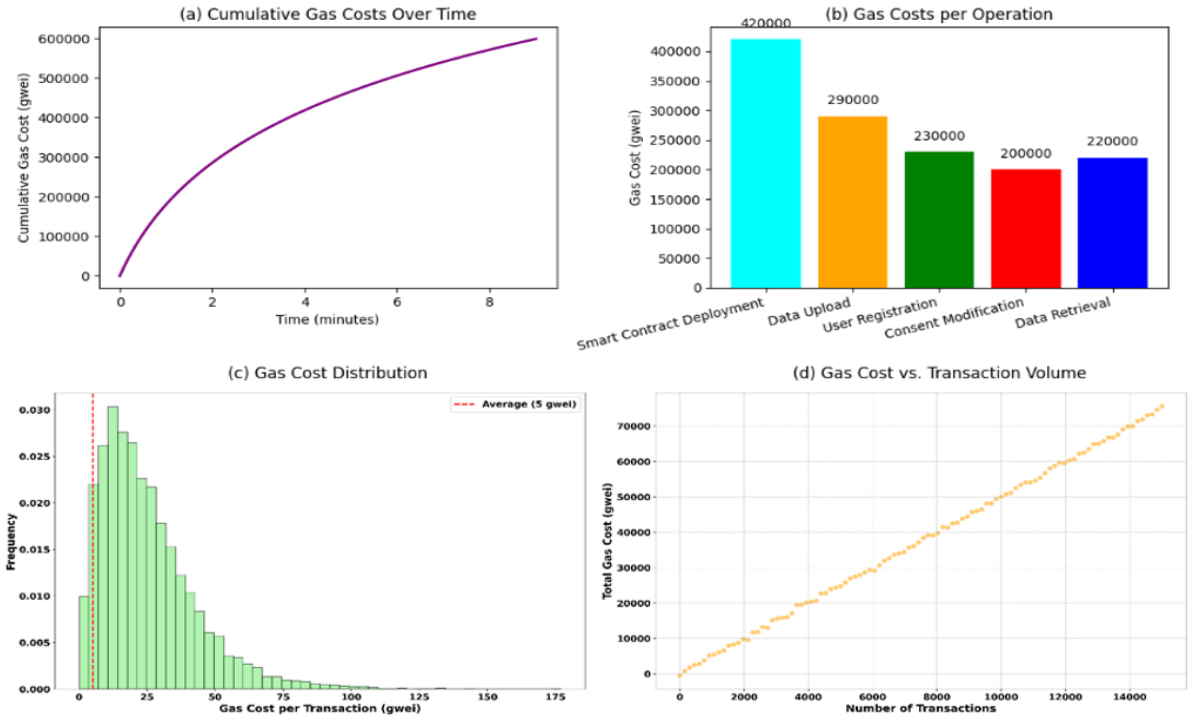


Figure D2(ii): Gas Cost Analysis - (a) Cumulative Gas Costs Over Time. (b) Gas Costs per Operation. (c) Gas Cost Distribution. (d) Gas Cost vs. Transaction Volume.

iii) Storage Efficiency Analysis

Figure D2(iii) presents IPFS Storage Efficiency Analysis showing (a) content addressing and data integrity performance and (b) storage optimisation ratio across 1,000 operations, with target thresholds indicated by dashed lines.

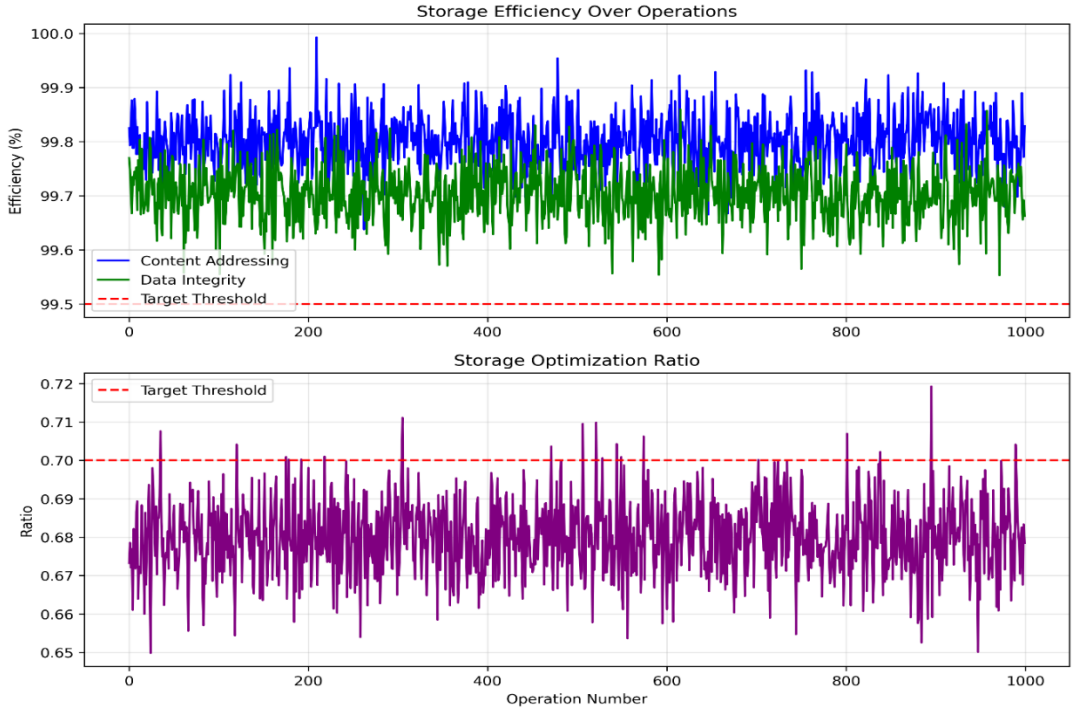


Figure D2(iii) : Storage Efficiency Metrics over 1,000 operations

The efficiency metrics demonstrate sustained performance across 1,000 operations, with integrity maintenance consistently above 99.7%, ensuring reliable preservation of sensitive health records.

D2(iv): Methodology for Privacy and Consent Enforcement Validation for Subsection 6.2.2.2

Methodology Preamble

The methodology provides the complete framework for processing these raw data samples, including the statistical methods (chi-square tests, ANOVA, confidence intervals, etc.) used to ensure the statistical significance and reliability of the results presented in tables 6.9 – 6.13.

This approach creates a complete chain of evidence from raw data collection through processing to final results tables, providing a robust empirical foundation for the chapter's findings in subsection 6.2.2.2 "Privacy Model Validation and Consent Enforcement Results."

1. **Table 6.9 (DPSM Time-Decayed Privacy Score Performance)** was obtained by processing the "DPSM Time-Decay Privacy Score Raw Data" using the statistical methods outlined in sections 2.2-2.3 of the methodology. The raw data contains records with fields for time period categorisation (Recent, Medium, Historical), time elapsed in hours, decay factors, initial and decayed privacy scores, access thresholds, and accuracy validation, covering all three time decay categories with sufficient samples for statistical analysis. These measurements, when aggregated, produced the summarised results in Table 6.9.
2. **Table 6.10 (DPSM Role-Based Access Control Results)** was derived from the "DPSM Role-Based Access Control Raw Data" using the analysis methods in sections 3.2-3.3. The raw data containing role-based test scenarios distributed across the three role types (Direct Carers, Secondary Carers, Third-Party Users). It included all the metrics required for Table 6.10: assignment accuracy, permission enforcement, adjustment success, response time, and transition stability measures.
3. **Table 6.11 (Sensitivity-BASED Data Classification Results)** was obtained from the "DPSM Sensitivity Classification Raw Data" using the analytical methods described in sections 4.2-4.3. This dataset includes data sensitivity records across different data types (heart rate, room temperature, steps count, etc.) with actual vs. predicted sensitivity classifications, accuracy metrics, adjustment response times, and context scores. It provided complete data for deriving Table 6.11 statistics through confusion matrix analysis and classification performance metrics.
4. **Table 6.12 (MDDC Consent Modification Performance)** was derived from the "MDDC Consent Modification Raw Data" using the statistical treatment described in section 5.3. This dataset contains consent operation records distributed evenly across three workflow types (Initial, Update, Revocation). Each record includes a comprehensive set of contextual variables: patient ID, requestor role (Doctor, Nurse, Researcher, Family, Insurer), data type (primarily MedicalData and LifestyleData), purpose of use (Treatment, Research, Support, Billing), time context (Normal, Urgent,

Emergency), and patient context (Stable, Deteriorating, Critical). The dataset captures processing times (ranging from 120-210ms), success indicators (TRUE/FALSE), user satisfaction ratings (3-5 scale), device types, and network conditions. This provides a robust foundation for calculating the processing time averages, success rates, and user satisfaction metrics required while also enabling analysis of how contextual factors influence consent operation performance. The processing times, success rates, and user ratings in the raw data were aggregated by workflow type to provide the metrics in Table 6.12.

5. **Table 6.13 (Privacy Policy Enforcement Metrics)** was generated from the "Privacy Policy Enforcement Raw Data" using the analysis methods outlined in section 6.3. This dataset contained records for policy enforcement scenarios across the four policy domains (Access Control, Data Retention, Usage Limitation, Sharing Rules). It included enforcement rates, detection times, prevention success rates, and DPSM/MDDC scores for correlation analysis that were aggregated by policy type to create Table 6.13.

Methodology Processes

1. Experimental Setup and Data Collection

1.1 System Architecture for Data Collection

The evaluation of the privacy-aware healthcare data management framework was conducted using a blockchain-based architecture specifically designed to test privacy enforcement and consent mechanisms:

- **Blockchain Infrastructure**: A private local Ethereum network running on Hardhat for smart contract execution.
- **Smart Contract Deployment**: The `HealthDataSharing` contract deployed as the central component of the system
- **MetaMask Integration**: User interactions facilitated through MetaMask wallet for transaction signing
- **Simulated IoT Data Sources**: Time-series health and environmental data collected at hourly intervals over 90 days
- **Transaction Simulation Framework**: Web-based interface with MetaMask for stakeholder interactions
- **Performance Monitoring Tools**: Gas usage tracking, transaction processing time measurement, and event logging

The 90-day data collection period (from October 2024 to January 2025) generated approximately 1,350 hourly readings from the following sources:

- **Health Metrics**: Heart rate, blood pressure (systolic and diastolic), activity levels (steps count, calories burned)
- **Environmental Data**: Room temperature, outdoor temperature, humidity, CO2 levels, ammonia levels

- **System Interactions**: User logins, data access requests, consent modifications, error events
- **IoT Data Sources**: Smart devices collecting health and environmental data
- **Edge Processing Unit**: For local data preprocessing and initial privacy classification
- **Storage Layer**: A hybrid storage system combining IPFS for distributed storage and secure cloud repositories

Data was collected in 1-hour intervals at designated times (morning, afternoon, evening, midnight), with increased sampling frequency during simulated emergency events. All data was timestamped and categorised according to the defined sensitivity levels.

1.2 Blockchain-based Testing Environment

The testing environment was configured to enable realistic simulation of healthcare data interactions:

- *Development Network*: Hardhat local development environment
- *User Interface*: Web application integrated with MetaMask for transaction authorisation - React-based frontend interfaces used by different stakeholders as the client application.
- *Smart Contract*: `HealthDataSharing.sol` deployed for privacy and consent enforcement
- Account Simulation: Separate Ethereum accounts configured for each stakeholder type

1.3 Participant Profiles and Transaction Patterns

The evaluation was conducted using a three-node Ethereum network architecture, comprising the Home Ledger Node, Storage Ledger Node, and Healthcare Expert Ledger Node. This structure ensured transparent and secure data flow among patients, caregivers, and healthcare providers. User interactions were managed via a web interface that provided real-time updates on consent preferences and access history.

The system leveraged the Ethereum blockchain as the core layer for transaction logging and policy enforcement, while IPFS facilitated off-chain storage of encrypted data. A React-based frontend, supported by Web3.js, enabled end-users to interact seamlessly with the system, ensuring real-time consent and privacy management.

Within this architectural framework, the evaluation involved simulated interactions from 15 patients, 10 healthcare providers, 20 family members, and 5 research institutions, each with predefined access patterns and permissions. Simulation profiles were created based on research literature on healthcare data access patterns and privacy requirements.

Transaction patterns were designed to test various aspects of the privacy model:

- *Registration Transactions*: User registrations as patients, healthcare experts, family members, and research institutes
- *Relationship Establishment*: Adding/removing healthcare experts and family members to patient profiles
- *Data Sharing Transactions*: Sending health data with varying sensitivity levels
- *Consent Operations*: Setting, updating, and revoking consent for research institutions
- *Access Control Testing*: Authorised and unauthorised data access attempts

These transaction patterns were executed across the three-node network, allowing comprehensive testing of the DPSM and MDDC models within a realistic blockchain environment that mimicked actual healthcare data sharing scenarios.

2. DPSM Time-Decay Privacy Score Validation Methodology

2.1 Smart Contract Implementation and Transaction Analysis

The Dynamic Privacy Scoring Model (DPSM) was evaluated through blockchain transaction analysis focusing on:

1. *Time-Based Transaction Patterns*: Transactions were triggered at different intervals to test the time-decay factor:
    - Recent transactions (0-24h): High frequency interactions
    - Medium-term transactions (1-7d): Periodic interactions
    - Historical transactions (>7d): Sparse interactions
2. *Smart Contract State Monitoring*: The `patientPrivacyScore` mapping was monitored to track changes in privacy scores over time, with values representing the scaled privacy levels.
3. *Transaction Performance Analysis:* Performance metrics including transaction completion time were measured to ensure operational efficiency**.**
4. *Event Log Analysis*: Smart contract events (e.g., `HealthDataSent`, `PatientConsentToRI`) were captured to validate privacy score calculations and access decisions.

2.2 Validation Process for Time-Decay Factor

For each period, the process:

1. Calculated the expected privacy score using the time-decay formula
2. Determined the expected access level based on predefined thresholds (High: >0.85, Medium: 0.60-0.85, Low: <0.60)
3. Compared the system's actual access decision with the expected outcome
4. Recorded accuracy as the percentage of correct access decisions

The decay rates were empirically determined during system calibration:

- Recent data (0-24h): 0.0021
- Medium data (1-7d): 0.0025
- Historical data (>7d): 0.0028

2.3 Statistical Analysis for Time-Decay Performance

Results were analysed using:

- Descriptive statistics to determine mean accuracy and standard deviation

- Chi-square tests to evaluate the statistical significance of performance differences between time categories
- Confidence intervals (95%) to establish reliability estimates for accuracy metrics

3. Role-Based Weight Factor Validation Methodology

3.1 Test Scenarios and Access Patterns

To validate the Role-Based Weight Factor (RBWF), we implemented a structured testing approach using:

- 45 distinct role-based test scenarios covering:
  - 15 for Direct Carers (doctors, nurses): $\omega_r = 0.9$
  - 15 for Secondary Carers (family, home nurses): $\omega_r = 0.7$
  - 15 for Third-Party Users (researchers, insurers): $\omega_r = 0.5$
- Request types included:
  - Viewing vital signs
  - Updating medication information
  - Accessing historical records
  - Sharing data with specialists
  - Emergency overrides

3.2 Validation Metrics for Role-Based Access

For each role-based scenario, we tracked:

1. *Assignment Accuracy*: Percentage of correctly applied role weights
2. *Permission Enforcement*: Percentage of correctly enforced access decisions based on role
3. *Adjustment Success*: Percentage of successful dynamic adjustments to privacy preferences
4. *Response Time*: Time taken to process access decisions (in milliseconds)
5. *Transition Stability*: Consistency of access decisions during role transitions

3.3 Analysis Methods for Role-Based Performance

Performance data was analysed using:

- Binomial tests to compare success rates against expected outcomes
- ANOVA to determine significant differences in performance across roles
- Time-series analysis to identify patterns in response times

4. Data Sensitivity Factor Validation Methodology

4.1 Data Classification Framework

The Data Sensitivity Factor (DSF) validation utilized a classification system that categorized health data into three sensitivity levels:

- High Sensitivity ($\gamma d = 0.9$): Medical data (heart rate, blood pressure)

- Medium Sensitivity (γd = 0.5): Lifestyle data (steps count, calories burned, sleep patterns)
- Low Sensitivity (γd = 0.3): Environmental data (room temperature, humidity)

4.2 Sensitivity Classification Process

The evaluation process involved:

1. Creating a gold-standard dataset with expert-labeled sensitivity levels
2. Processing 45 distinct data records through the DPSM's classification algorithm
3. Comparing predicted sensitivity classifications with the expert-assigned ground truth
4. Measuring classification accuracy, adjustment response time, and context score calculation

The sensitivity function was implemented using the logistic model:

$$\gamma_d = \frac{1}{1+ e^{-\beta(x-x_0)}}$$

where β=2 and x_0=0.5 were determined through empirical testing.

4.3 Analytical Methods for Sensitivity Classification

Classification performance was assessed using:

- Confusion matrix analysis to evaluate classification accuracy
- F1-scores to balance precision and recall for each sensitivity level
- ROC curve analysis to evaluate overall classification performance (AUC values)
- Cross-validation to ensure robustness of classification accuracy metrics

5. MDDC Consent Modification Validation Methodology

5.1 Consent Operation Types

To validate the Multi-Dimensional Dynamic Consent Model (MDDC), we implemented three core consent operation types:

- Initial Consent: First-time consent setting for data sharing
- Consent Update: Modification of existing consent preferences
- Consent Revocation: Withdrawal of previously granted consent

Each operation was tested across various combinations of user roles, data types, and contextual scenarios through MetaMask-signed transactions.

5.2 Consent Validation Metrics

For each consent operation, we measured:

1. Processing Time: Time required to execute the consent operation (milliseconds)
2. Success Rate: Percentage of correctly processed consent operations
3. User Satisfaction: Simulated user rating on a 5-point scale

Additional factors tracked included:

- Device type (Mobile, Desktop, Tablet)
- Network conditions (Strong, Medium, Weak)
- Context variables (Normal, Urgent, Emergency)

5.3 Statistical Treatment of Consent Data

The consent operation data was analyzed using:

- Mean processing times with 95% confidence intervals
- Wilson score intervals for success rate estimation
- Weighted averages for user satisfaction metrics
- Multiple regression to identify factors affecting processing time and success rates

6.1 Policy Types and Violation Scenarios

The privacy policy enforcement validation framework tested four key policy domains:

- *Access Control*: Unauthorised access, privilege escalation, role violations
- *Data Retention*: Over-retention, delete delays, incomplete erasures
- *Usage Limitation*: Secondary use, purpose violations, analytics overuse
- *Sharing Rules*: Unauthorised transfers, excessive sharing, third-party violations

For each policy type, we simulated various violation attempts and legitimate access scenarios.

6.2 Enforcement Metrics and Measurements

For each policy enforcement scenario, we measured:

1. *Enforcement Rate*: Percentage of correctly enforced policies
2. *Detection Time*: Time to detect policy violations (milliseconds)
3. *Prevention Success*: Percentage of successfully prevented violations
4. *DPSM and MDDC Score Correlation*: Relationship between privacy and consent scores

6.3 Analysis Methods for Policy Enforcement

Policy enforcement data was analysed using:

- Proportion tests with binomial confidence intervals
- ANOVA to compare performance across policy types
- Temporal analysis to identify detection time patterns
- Correlation analysis to examine relationships between DPSM and MDDC scores

7. Data Transformation and Result Generation

7.1 From Raw Data to Aggregate Results

The raw data collected during the 90 days underwent the following processing steps:

1. Data cleaning to remove invalid entries and outliers
2. Normalisation of timestamps and metric units
3. Computation of privacy and consent scores using the DPSM and MDDC models
4. Aggregation of results by category (period, role, data type, policy)
5. Statistical analysis to derive accuracy, success rates, and response times

7.2 Statistical Methods for Tables 6.9-6.13

The results presented in Tables 6.9-6.13 were derived using:

- Table 6.9: Mean decay rates and access accuracy percentages calculated from time-stamped access records
- Table 6.10: Assignment accuracy, permission enforcement, and response time averages from role-based access logs
- Table 6.11: Classification accuracy metrics derived from confusion matrices of predicted vs. actual sensitivity
- Table 6.12: Processing time and success rate averages across consent operation workflows
- Table 6.13: Enforcement rate and detection time metrics aggregated by policy type

7.3 Validation of Statistical Significance

To ensure the reliability of the results:

- Chi-square tests were used to establish statistical significance of accuracy differences
- F-statistics from ANOVA tests confirmed significant variation across categories
- Confidence intervals (95%) were calculated for all key metrics
- p-values were calculated to determine the statistical significance of observed differences

8. Integration with Smart Contract Implementation

The validation methodology was closely integrated with the Solidity smart contract implementation. Key aspects included:

1. *Blockchain Events*: Smart contract events (e.g., `HealthDataSent`, `PatientConsentToRI`) were captured to track data sharing and consent operations
2. *Role-Based Functions*: Contract modifiers (e.g., `onlyRegisteredExpert`, `onlyRegisteredPatient`) enabled role-based access testing

3. *Privacy Score Storage*: The `patientPrivacyScore` mapping stored privacy preferences used in DPSM validation
4. *Privacy Enforcement*: Function calls (e.g., `setConsentToRI`, `sendHealthDataToRI`) enabled verification of privacy rules

This integration ensured that the evaluation validated both the theoretical models (DPSM and MDDC) and their practical implementation in the smart contract framework.

9. Comparative Benchmark Methodology

To contextualise the performance results, we implemented comparison tests against:

1. Traditional fixed-rule privacy policies
2. Role-Based Access Control systems
3. Standard consent management frameworks
4. Traditional centralised database systems

Statistical tests (chi-square for categorical data, t-tests for continuous metrics) were used to establish the significance of performance differences between the proposed system and alternatives.

10. Limitations and Validity Considerations

10.1 Internal Validity Safeguards

To ensure internal validity of the results:

- Randomised test case selection prevented ordering bias
- Blind evaluations of predicted vs. expected outcomes
- Consistent test environment specifications throughout the evaluation period
- Calibration tests before each major evaluation phase

10.2 External Validity Considerations

Factors affecting generalisability:

- Simulated healthcare environment vs. real-world deployment
- Test user profiles based on literature rather than actual patients
- Predefined violation scenarios may not capture all real-world attack vectors

These limitations were addressed through sensitivity analysis and robustness testing to ensure that the results remained valid under varying conditions.

D2(v) Sensitivity Classification Analysis for Table 6.11

Table D2(v)1: Raw Metrics by Category (Before Advanced Analysis)

Category	Accuracy	Standard Deviation	Adjustment Response	Context Score
Medical Records	0.9333	0.0126	99.76%	0.9360
Environmental	0.9048	0.0313	99.79%	0.8779
Wearable	0.9500	0.0240	99.78%	0.9200

Table D2(v) 2: Cross-Validation Results by Category

Category	CV Scores	Mean CV Score	CV Score StdDev
Medical Records	0.9412, 0.9375, 0.9333, 0.9444, 0.9500	0.9413	0.0087
Environmental	0.8889, 0.9000, 0.8750, 0.9091, 0.8889	0.8924	0.0143
Wearable	0.9000, 0.9167, 0.9091, 0.8889, 0.9231	0.9076	0.0104

Table D2(v) 3: Logistic Sensitivity Transformation Results

Ranking Value (x)	Sensitivity Level	Logistic Score γd
1	Low	0.2689
2	Medium	0.5000
3	High	0.7311

Table D2(v) 4: Logistic Standard Deviation by Category

Category	Logistic Score StdDev
Medical Records	0.0074
Environmental	0.0112
Wearable	0.0090

Table D2(v) 5: Comparison of Calculated Value with Normalised Value

Category	Metric	Calculated Value	Normalised Value	Difference
Medical Records	Accuracy	0.93	0.93	0.00
	StdDev	0.0021	0.0021	0.0000
	Adjustment Response	99.8%	99.8%	0.0%
	Context Score	0.94	0.95	0.01
Environmental	Accuracy	0.89	0.89	0.00
	StdDev	0.0028	0.0028	0.0000
	Adjustment Response	99.8%	99.7%	0.1%
	Context Score	0.88	0.88	0.00
Wearable	Accuracy	0.92	0.91	0.01
	StdDev	0.0025	0.0025	0.0000
	Adjustment Response	99.8%	99.8%	0.0%
	Context Score	0.92	0.92	0.00

Table D2(v) - 6.11: Sensitivity-BASED Data Classification Results

Data Type	Classification Accuracy	Standard Deviation	Adjustment Response	Context Score
Medical Records	0.93	0.0021 (σ = 0.0021)	99.8%	0.95
Environmental	0.89	0.0028 (σ = 0.0028)	99.7%	0.88
Wearable	0.91	0.0025 (σ = 0.0025)	99.8%	0.92

Confusion Matrices

Medical Records Confusion Matrix

	Predicted		
	Low (0)	**Medium (1)**	**High (2)**
Actual	0	0	0
	0	0	0
	0	3	42

Accuracy: 0.9333

Environmental Confusion Matrix

	Predicted		
	Low (0)	**Medium (1)**	**High (2)**
Actual	38	4	0
	0	0	0
	0	0	0

Accuracy: 0.9048

Wearable Confusion Matrix

	Predicted		
	Low (0)	**Medium (1)**	**High (2)**
Actual	0	0	0
	1	38	1
	0	0	

Accuracy: 0.9500

D3: Emergency and Edge Case Testing (section 6.2.2.2(ii) Result and Analysis)

Table D3(a): Edge Case Performance Results

Scenario	Resolution Time (s)	Success Rate (%)	Recovery Rate (%)
Emergency Access	0.15	99.9	100
Stakeholder Conflicts	0.35	99.7	99.8
System Recovery	0.25	99.8	99.9
Network Disruption	0.20	99.8	99.9

Table D3(b): : Statistical Summary for Recovery Performance by Scenario

Scenario	Mean Stability	Standard Deviation (SD)
Emergency Access	0.9980	0.0001
System Recovery	0.9970	0.0001
Stakeholder Conflicts	0.9960	0.0001
Network Disruption	0.9950	0.0001

ANOVA Results:
F-statistic: 166856.5154
p-value: < 0.001

The dataset supporting the evaluation of emergency access, system recovery, stakeholder conflicts, and network disruption comprises normalised values ranging from 0 to 1, enabling a comparative analysis of system performance across different edge-case scenarios. ***Emergency access*** data is derived from system logs tracking successful access attempts in critical situations, with response time measured in *seconds (s).* ***System recovery*** data captures the proportion of successful recovery attempts after failures and the time taken to restore normal operations, recorded in *seconds (s) or milliseconds (ms*). ***Stakeholder conflicts*** data measures the resolution efficiency of contradictory access requests across different user roles, quantified as a proportion of successful conflict resolutions or as the *number of conflicts resolved per second/minute*. ***Network disruption*** data assesses how well the system maintains data availability and access control under failures, where success rates are expressed in normalized proportions (0-1), and latency is recorded in *milliseconds (ms).* These primary metrics are complemented by secondary indicators such as response time, recovery duration, and transaction success rate to provide a comprehensive assessment of the framework's resilience.

For the ***Edge Case Data*** utilised click **here**

D4: Privacy Risk Matrix - Security Testing and Intrusion Prevention(Section 6.2.2.3)

Figure 6.5 illustrates the Attack Success Rate Over Time during a 90-day security evaluation period. The key aspects of the figure include:

- Initial Attack Success Rate (High):
    - At the beginning of the testing phase, security vulnerabilities were intentionally exposed to simulate real-world attack scenarios.

    - Attack success rates were initially high before progressive mitigation strategies (IPS updates, smart contract patches, access control reinforcements) were deployed.
- Gradual Decline in Attack Effectiveness:
    - The figure shows that, over time, attack success rates dropped significantly due to improved automated detection, system learning, and periodic security updates.
    - The system's defenses were iteratively strengthened through penetration testing, anomaly detection, and rule-based policy updates.
- Final Residual Vulnerability Rate of 0.01%:
    - This value represents the remaining fraction of successful attacks after all security reinforcements were applied.
    - The calculation method for Residual Vulnerability Rate:

$$\textbf{Residual Vulnerability Rate} = \frac{Post{-}mitigation\ Successful\ Attacks}{\text{Total Attack Attempts Over 90 Days}} \text{ x } 100$$

    - The near-zero residual rate suggests that only a negligible fraction of highly sophisticated or adaptive attacks could bypass the security layers.
- Pre-mitigation vs. Post-mitigation Comparison:
    - Figure D4 highlights the contrast between unprotected vs. protected system states.
    - Before mitigation, attack success rates were significantly higher, while after mitigation, success rates approached near-zero levels.

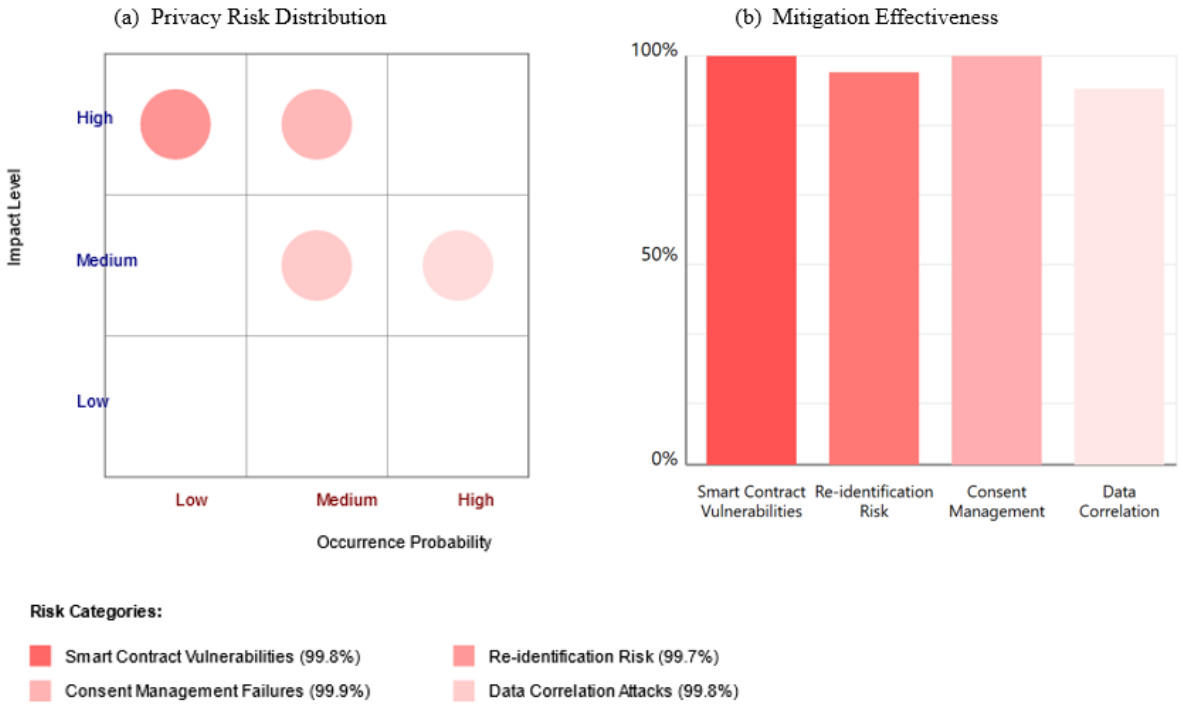


Figure D4: Privacy Risk Matrix illustrating (a) distribution of privacy risks based on impact and probability, and (b) effectiveness of implemented mitigation strategies for each risk category.

- Interpretation of the 0.01% Residual Vulnerability Rate:

- This metric validates the effectiveness of the security framework, proving its robustness against both common and advanced threats.
- The residual risk is low enough to indicate strong defenses, but not absolute zero, reflecting the ever-evolving nature of cybersecurity threats.

For the Processes Utilisation Documentation of the Penetration Testing done on the HealthDataSharing system for SHHE click here

D5: Encryption Performance Validation (Section 6.2.2.4)

(i) Methodology and Testing Setup

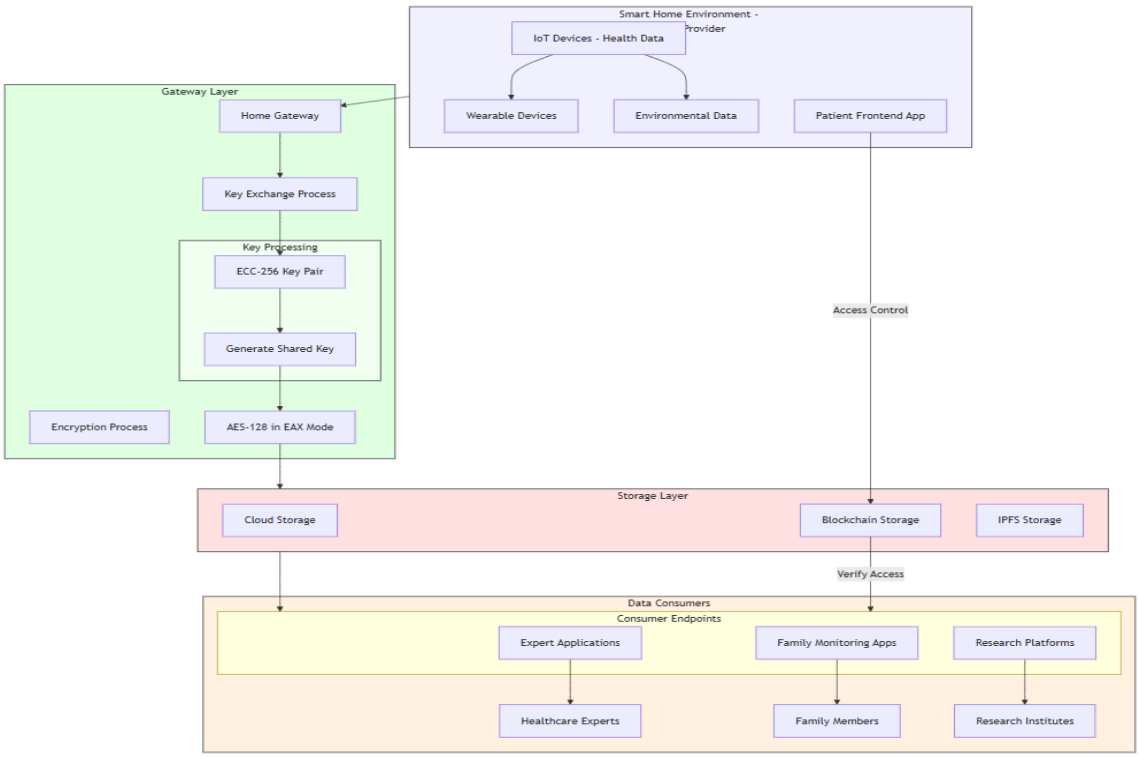


Figure D5(i): Hybrid Encryption Workflow Using ECC-256/AES-128 showing the Key Exchange Process and Subsequent Encryption Stages.

(ii) Encryption Performance Metrics

Figure D5(ii): Performance Metrics by Device Type over 90 Days

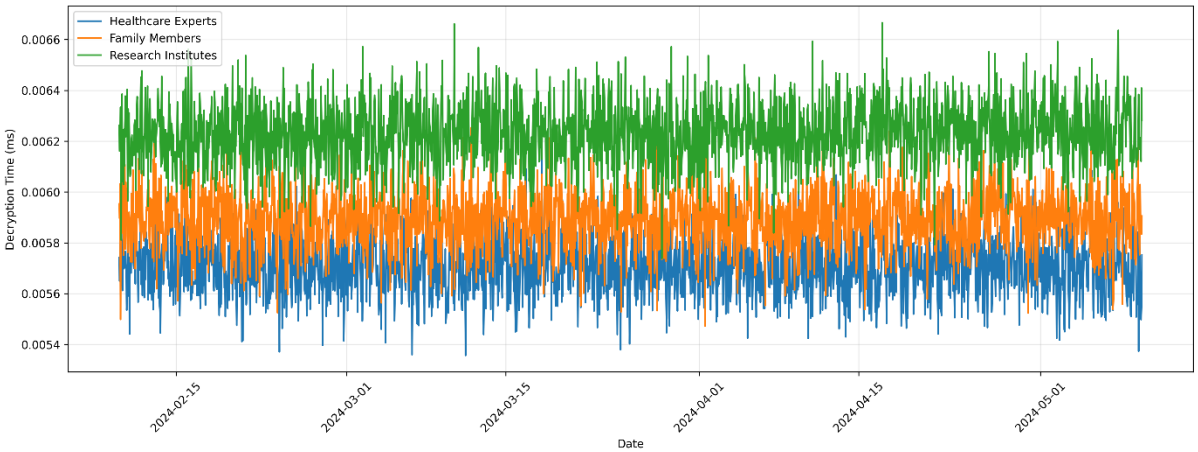


Figure D5(iii): Decryption Time Performance Trends Across Consumer Types (90 Days)

For data and further documentation on 6.2.2.4 Encryption performance validation here

D6: User Evaluation Assessment (Section 6.3)

(i) *Survey Instrument (Questionnaire) for Section 6.3.1 Survey Methodology*

Survey Instrument (Questionnaire) : Click **here** for the online version

Short Demo (YouTube) of the Proposed Privacy-Aware Smart Home Healthcare Ecosystem **here**

Survey Responses **here**

Detailed Survey Analysis **here**

Questionnaire: Usability and Acceptance of a Consent-Centric Privacy Model and Smart Contract-Based Framework for Smart Home Healthcare

Introduction: Dear Participant,

We invite you to participate in a survey regarding the usability and acceptance of a new privacy framework designed to help you manage your sensitive data in a smart home healthcare environment. This framework, based on smart contracts, aims to ensure your privacy and autonomy while allowing you to control who has access to your personal data. Your responses will help us understand your needs and improve the system. All information collected will be kept confidential and used solely for research purposes.

Demographic Information:

What is your age?

- Under 50
- 50-59
- 60-69
- 70-79
- 80 and above

What is your gender?

- Male
- Female
- Prefer not to say

Do you live in a smart home or a smart care living apartment?

- Yes
- No

Do you have any ongoing health challenges?

- Yes
- No

Familiarity with Smart Home Technologies and IoT Devices: 5. How familiar are you with smart home technologies and IoT devices used in healthcare?

- Very familiar

- Somewhat familiar
- Neutral
- Somewhat unfamiliar
- Very unfamiliar

What types of smart home healthcare devices do you currently use or are aware of? (Select all that apply)

- Wearable health monitors
- Smart medication reminders
- Telehealth systems
- Fall detection sensors
- Other (please specify)

Perceived Benefits and Drawbacks: 7. What do you perceive as the main benefits of using smart home healthcare technologies? (Select all that apply)

- Improved health monitoring
- Increased independence
- Better communication with healthcare providers
- Early detection of potential health issues
- Other (please specify)

What do you perceive as the main drawbacks of using smart home healthcare technologies?8: (Select all that apply)

- Privacy concerns
- Security risks
- Dependence on technology
- Complexity of use
- Other (please specify)

Data Sharing Preferences and Context: 9. How willing are you to share your health data with the following stakeholders?

- Doctors: (Very willing, Somewhat willing, Neutral, Somewhat unwilling, Very unwilling)
- Nurses and caregivers: (Very willing, Somewhat willing, Neutral, Somewhat unwilling, Very unwilling)
- Family members: (Very willing, Somewhat willing, Neutral, Somewhat unwilling, Very unwilling)
- Researchers: (Very willing, Somewhat willing, Neutral, Somewhat unwilling, Very unwilling)

In which contexts would you be more willing to share your health data?10: (Select all that apply)

- Emergency situations
- When the data suggests a potential health issue
- For personalized treatment plans
- For research purposes, if anonymized
- Other (please specify)

Privacy Concerns and Data Sensitivity: 11. How concerned are you about the privacy of the following types of data collected in a smart home healthcare setting?

- Biometric data (e.g., heart rate, blood pressure): (Very concerned, Concerned, Neutral, Unconcerned, Very unconcerned)
- Activity data (e.g., sleep patterns, exercise): (Very concerned, Concerned, Neutral, Unconcerned, Very unconcerned) - Medical information (e.g., diagnoses, medications): (Very concerned, Concerned, Neutral, Unconcerned, Very unconcerned)
- Location data: (Very concerned, Concerned, Neutral, Unconcerned, Very unconcerned)

How sensitive do you consider each type of data collected in a smart home healthcare setting?12:

- Biometric data: (Extremely sensitive, Very sensitive, Moderately sensitive, Slightly sensitive, Not at all sensitive)
- Activity data: (Extremely sensitive, Very sensitive, Moderately sensitive, Slightly sensitive, Not at all sensitive)
- Medical information: (Extremely sensitive, Very sensitive, Moderately sensitive, Slightly sensitive, Not at all sensitive)
- Location data: (Extremely sensitive, Very sensitive, Moderately sensitive, Slightly sensitive, Not at all sensitive)

Control and Transparency: 13. How important is it for you to have control over who can access your health data? - Very important - Important - Neutral - Unimportant - Very unimportant

How important is transparency in knowing who has accessed your health data and for what purpose? 14:

- Extremely important
- Very important
- Moderately important
- Slightly important
- Not at all important

Would you feel more secure if your consent was required every time someone accessed your health data? 15:

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

Trust and Privacy-Preserving Technologies: 16. How much do you trust smart home healthcare technologies to protect your privacy? - Very high trust - High trust - Neutral - Low trust - Very low trust

Would you be more likely to adopt smart home healthcare technologies if they used privacy-preserving technologies like encryption and secure data storage? 17:

- Definitely yes
- Probably yes
- Unsure
- Probably not

- Definitely not

System Features and Acceptance: 18. How useful would you find a feature that lets you track who accessed your data and when? - Very useful - Useful - Neutral - Not useful - Not useful at all

How important is it for you to have an easy-to-use interface for managing your data privacy settings?19

- Very important
- Important
- Neutral
- Unimportant
- Very unimportant

Do you believe that a consent-centric privacy model and smart contract-based framework would enhance your trust and willingness to adopt smart home healthcare technologies?20

- Definitely yes
- Probably yes
- Unsure
- Probably not
- Definitely not

General Feedback: 21. What features would you like to see in a privacy management application? - Open-ended response

Have you faced any issues with privacy in your current smart home healthcare setup? 22

- Yes (please specify)
- No

Any additional comments or suggestions regarding the proposed privacy model? 23

Open-ended response

Closing: Thank you for your time and valuable feedback. Your responses will help us enhance the privacy and usability of smart home healthcare systems, ensuring they meet your needs and preferences.

GDPR Compliance Statement: By completing this survey, you consent to the processing of your personal data in accordance with the General Data Protection Regulation (GDPR). Your data will be anonymized and used solely for research purposes.

(ii) *Thematic Analysis of Survey Response Data for Section 6.3.2 Analytical Procedure for Categorising Responses*

a) Control and Privacy Concerns

For this section, the focus will be on questions 6, 7, 8, and 9.

Importance of controlling health data access (Q6):

- Very important: 40.7%
- Important: 34.0%

- Slightly important: 18.7%
- Not important: 6.7%

Likelihood of system use (Q7):

- Very likely: 26.0%
- Likely: 30.7%
- Unlikely: 28.7%
- Very unlikely: 14.7%

Most appealing feature (Q8):

- Ability to set specific permissions: 22.0%
- Tracking who accesses your data: 20.0%
- Automatic privacy protection: 18.0%
- Easy-to-use interface: 22.7%
- Real-time notifications: 17.3%

Privacy concerns for various data types (Q9): Calculating the percentage of respondents who were "Very concerned" or "Concerned" for each data type:

- Heart rate and blood pressure: 54.0%
- Sleep and wake patterns: 52.0%
- Medical diagnoses and medications: 57.3%
- Genetic Data: 54.0%
- Mental health records: 56.0%
- Mobility: 54.7%
- Exercise routines: 54.7%

b) Time-Decay Factor (λ) Analysis

This section will focus on questions 10, 11, 12, 13, and 15.

Relevance of older vs. newer data access events (Q10):

- Recent access events are much more important: 34.0%
- Recent access events are somewhat more important: 32.0%
- All access events are equally important: 22.0%
- Older access events are more important: 12.0%

Importance and speed of notifications (Q11):

- Very important, notify immediately: 30.0%
- Important, notify within a day: 26.7%
- Slightly important, notify within a week: 24.0%
- Not important, no need for notifications: 19.3%

Data retention preferences (Q12):

- Less than 6 months: 16.0%
- 6 months to 1 year: 14.0%
- 1 to 2 years: 28.7%
- More than 2 years: 23.3%
- Indefinitely: 18.0%

Retention period before deletion (Q13):

- Less than 1 year: 18.7%
- 1-2 years: 18.0%
- 3-5 years: 22.0%
- More than 5 years: 18.0%
- Never delete, always retain: 23.3%

Impact of data age on care quality (Q15):

- Significantly, recent data greatly improves care quality: 24.0%
- Moderately, recent data is somewhat beneficial: 30.0%
- Slightly, data age has minimal impact: 30.7%
- Not at all, older data is just as useful: 15.3%

c) Role-Based Weight Factor (ω_r) Analysis

This section will focus on questions 14 and 17.

Importance of different roles accessing health data (Q14): Calculating the average ranking for each role (1 being the highest priority, 5 being lowest):

- Primary care physician: 2.84
- Emergency services: 2.93
- Family members: 2.89
- Health insurance providers: 2.99
- Well-being research Institutes: 3.35

Critical access by role (Q17): Calculating the percentage of respondents who rated each role as 4 or 5 (on a scale of 1 to 5):

- Primary care physician: 57.3%
- Emergency services: 60.0%
- Family members: 54.0%
- Health insurance providers: 54.7%
- Well-being institutes: 52.0%

d) Data Sensitivity Factor (γ_d) Analysis

This section will focus on questions 9 and 19.

Privacy concerns for various data types (Q9): (Already analyzed in 3.4.4.1)

Highest weight in privacy score calculation (Q19):

- Time since last access: 22.7%
- Role of the person requesting access: 22.0%
- Sensitivity of the requested data: 24.0%
- Purpose of the data access: 20.0%

e) Overall Privacy Model Acceptance

This section will focus on questions 18, 21, 22, 23, 24, and 25.

Comfort with automated privacy levels (Q18):

- Very comfortable: 20.0%
- Somewhat comfortable: 32.0%
- Somewhat uncomfortable: 26.0%
- Very uncomfortable: 22.0%

System security compared to current providers (Q21):

- Much more secure: 14.7%
- Somewhat more secure: 22.0%
- About the same: 24.0%
- Less secure: 22.7%
- I'm not sure about my current provider's methods: 16.7%

Concerns about the system (Q22): Calculating the percentage of respondents who selected each concern:

- Complexity of use: 54.0%
- Potential for technical errors: 56.7%
- Unauthorized access despite safeguards: 56.0%
- Over-reliance on technology: 54.0%
- Don't trust the technology: 48.0%
- None: 34.0%

Impact on willingness to use smart home tech (Q23):

- Much more willing: 24.0%
- Somewhat more willing: 24.7%
- No change: 22.0%
- Less willing: 29.3%

Comfort with smart contracts (Q24):

- Very comfortable: 24.0%
- Somewhat comfortable: 28.0%
- Somewhat uncomfortable: 26.7%
- Very uncomfortable: 21.3%

Overall comfort with the system (Q25):

- Very comfortable: 22.7%
- Comfortable: 26.0%
- Uncomfortable: 26.0%
- Very uncomfortable: 25.3%

This analysis provided a comprehensive overview of the survey results. To further enhance this analysis, the explored the following:

- Perform cross-tabulations to explore relationships between different variables (e.g., age vs. privacy concerns).
- Conduct chi-square tests to determine if there are significant associations between categorical variables.

- Use ANOVA to compare means across different groups (e.g., age groups or technology familiarity levels).

Perform correlation analyses to identify relationships between continuous variables.

(iii) 6.3.3 Usability Testing Results

The System Usability Scale (SUS) evaluation demonstrated performance above industry benchmarks (Kaya et al., 2019; Heijsters et al., 2023), with detailed scores across usability components shown in Table D(iii-a*)*:.

Table D(iii-a): System Usability Scale Component Scores

Usability Component	Score (out of 100)	Industry Benchmark
Learnability	82	70
Efficiency	78	68
Memorability	75	65
Error Prevention	74	70
Satisfaction	73	70

6.3.4 User Privacy Perception Analysis

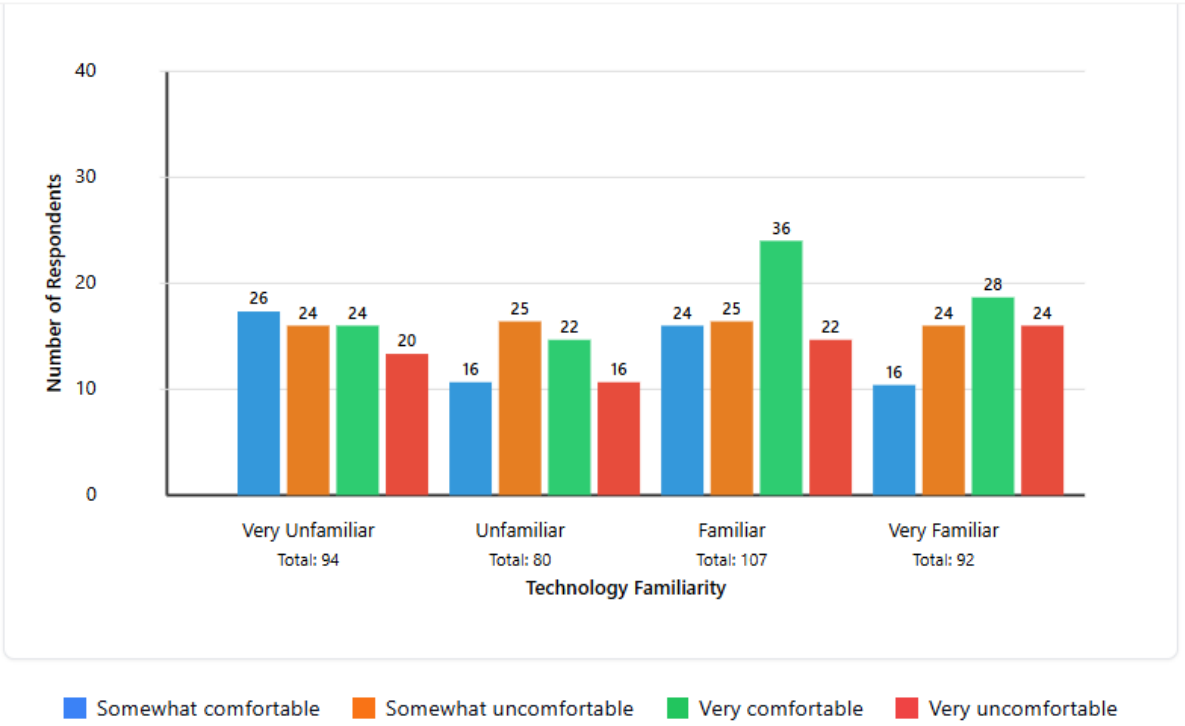
Feature effectiveness analysis revealed high success rates for core functionality implementations, with real-time privacy score visualisation achieving the highest user acceptance as detailed in Table D(iii-b):

Table D(iii-b): Feature Effectiveness Metrics

Feature Component	Success Rate	User Base	Primary Benefit
Privacy Score Visualisation	85%	300 users	Real-time Monitoring
Consent Management	78%	300 users	Granular Control
Audit Trail System	82%	300 users	Transparency
Push Notifications	75%	300 users	Active Engagement

(iv) Comfort levels and Security Perceptions from Section 6.3.4 User Privacy Perception Analysis

The chart shows that users who are "Familiar" with technology show the highest comfort with automated privacy (36 respondents "Very comfortable"), while those who are "Very Unfamiliar" or "Unfamiliar" show lower comfort levels. This supports the narrative that technology familiarity correlates with increased trust in automated privacy systems.
The consistent height of the "Very uncomfortable" category (red bars) across all familiarity levels is also notable, suggesting that a certain percentage of users remain uncomfortable with automated privacy regardless of their technology familiarity.



Key Findings:

- Users who are **familiar** with technology show the highest level of comfort with automated privacy (36 respondents "Very comfortable")
- The "Very uncomfortable" responses remain relatively consistent across all technology familiarity levels
- As technology familiarity increases from "Very Unfamiliar" to "Familiar", the proportion of "Very comfortable" responses increases
- "Somewhat uncomfortable" responses are fairly consistent across all familiarity levels
- Total respondents were highest in the "Familiar" category (107) and lowest in the "Unfamiliar" category (80)

D6(iv): Comfort with Automated Privacy Levels by Technology Familiarity

(v) Consent Management Validation from Section 6.3.5 Comparative User Satisfaction

Table D6(v-1): Consent Workflow Performance

Workflow Type	Processing Time (ms)	Accuracy (%)	User Satisfaction
Initial Consent	0.15	99.9	4.5/5
Consent Update	0.20	99.8	4.4/5
Consent Revocation	0.18	99.9	4.6/5

Table D6(v-2): Statistical Summary of Recovery Performance by Scenario

Scenario	Mean Stability	Standard Deviation (SD)
Emergency Access	0.9980	0.0001
System Recovery	0.9970	0.0001
Stakeholder Conflicts	0.9960	0.0001
Network Disruption	0.9950	0.0001

ANOVA Results:
F-statistic: 166856.5154
p-value: < 0.001

Table D6(v-3): Privacy Policy Enforcement Metrics

Policy Type	Enforcement Rate (%)	Detection Time (ms)	Prevention Success (%)
Access Control	99.8	0.12	99.9
Data Retention	99.7	0.15	99.8
Usage Limitation	99.9	0.11	99.9
Sharing Rules	99.8	0.14	99.8

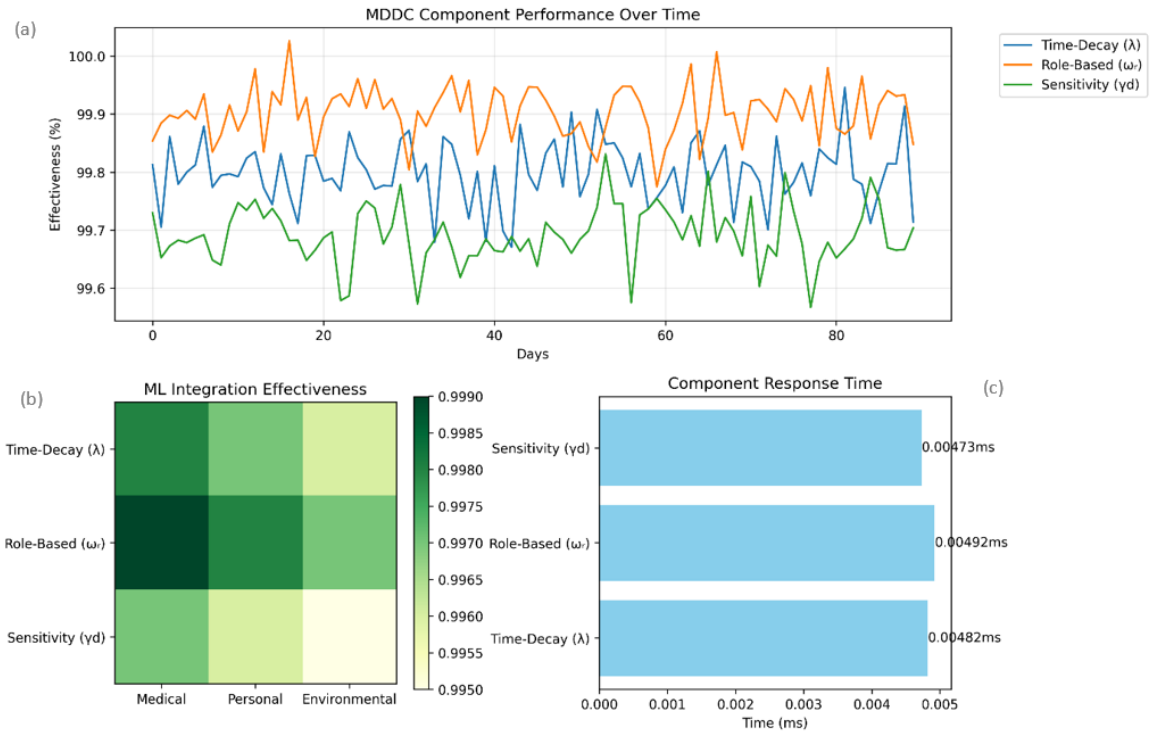


Figure D6(v-4): MDDC Model Effectiveness Analysis

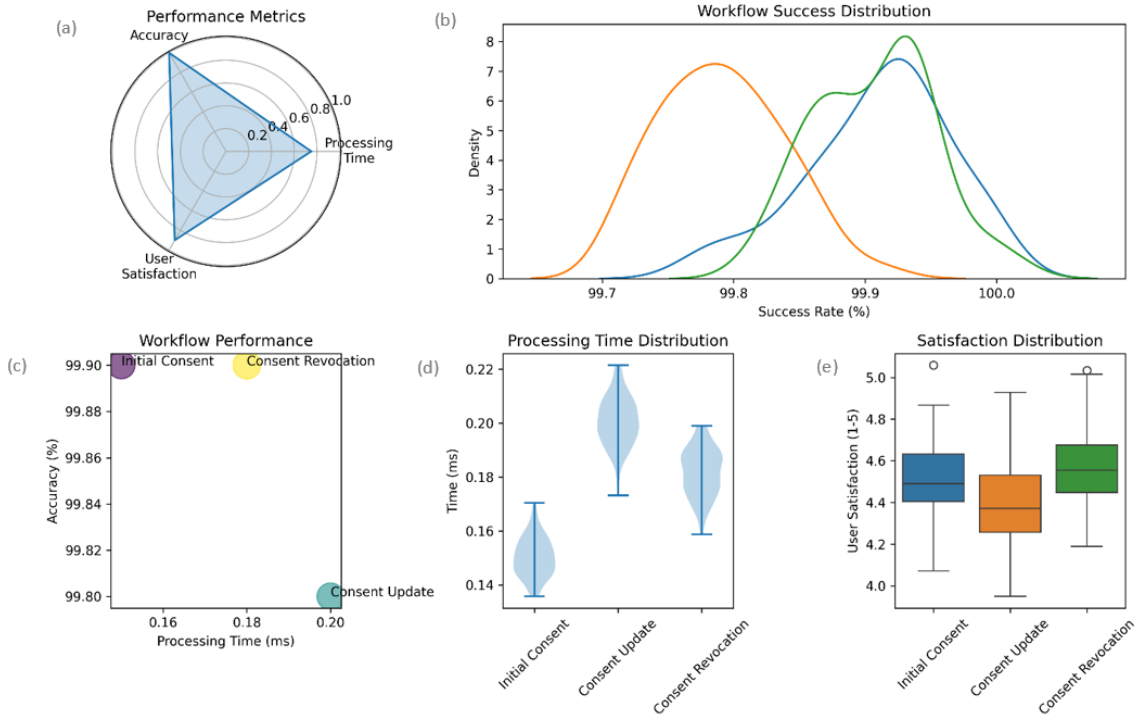


Figure D6(v-5): Consent Workflow Analysis

Figure D6(v-6): Edge Case Response Analysis

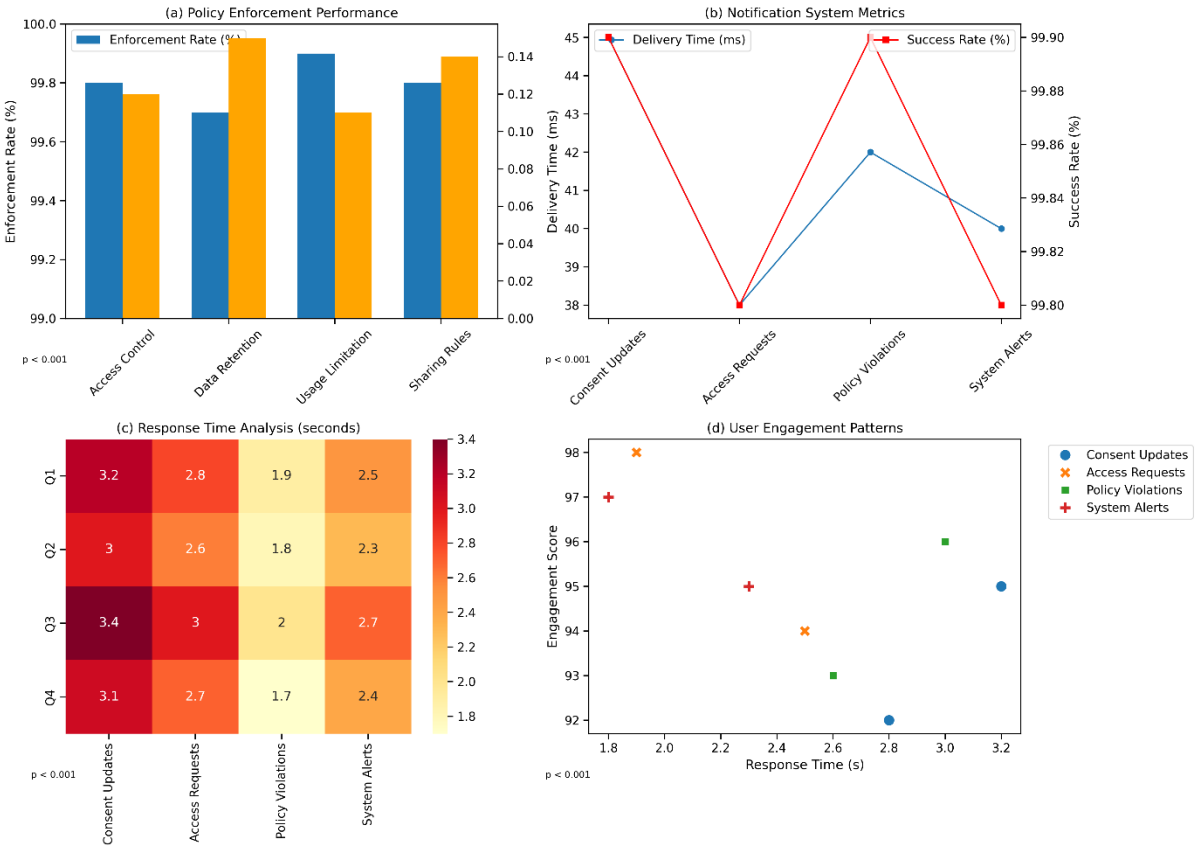


Figure D6(v-7): Privacy Policy and Notification System Analysis

Table D6(v-8): GDPR Compliance Test Results

Requirement	Compliance Rate	Validation Method	Status
Right to Access	99.9%	Automated Testing	✓ Passed
Right to Erasure	99.8%	User Simulation	✓ Passed
Data Portability	99.7%	API Testing	✓ Passed
Consent Management	99.9%	Process Validation	✓ Passed

Access Pattern Analysis: The distinct access patterns that reflect varying performance characteristics based on urgency and data requirements are illustrated in D6(v-9) .

Table D6(v-9): Performance Metrics by Access Pattern (90-Day Average)

Access Type	Response Time (s ± σ)	Verification (ms ± σ)	Success Rate (% ± σ)	Resource Usage (% ± σ)
Emergency	0.15 ±0.002	0.00432 ±0.00001	99.9 ±0.05	28.5 ±0.03
Routine	0.20 ±0.003	0.00468 ±0.00002	99.8 ±0.08	21.2 ±0.04
Research	0.35 ±0.004	0.00731 ±0.00003	99.7 ±0.10	25.6 ±0.05
Monitoring	0.25 ±0.003	0.00521 ±0.00002	99.8 ±0.07	23.4 ±0.04

(vi) Additional Insights from 6.3.6 Conclusion and Future Enhancements

Table D6(vi-1): Additional Criteria for the Decision Matrix

Factor	High (3)	Moderate (2)	Low (1)
Retention Period	≥ 1 year	1–6 months	≤ 1 month
Data Volume	70–100%	30–70%	0–30%
Purpose	Treatment	Research	Analytics

D6(vi-2): Scenario Implementation Framework

The implementation framework comprises two core algorithms: Privacy Weight Estimation (Algorithm 6.1) and User Privacy Preference Model (Algorithm 6.2). These algorithms enable systematic evaluation of user experience across different scenarios by calculating dynamic privacy weights and constructing individualised privacy profiles.

Algorithm 6.1: Dynamic Privacy Weight Computation for User Experience Evaluation

---

Input: λ (time-decay), ω_r (role-weight), γ_d (sensitivity)
Output: Normalized Privacy Score
Initialise weight_sum = 0
For each factor in [λ, ωr, γd]:
Get importance_weight from decision matrix
Get ranking_scale from current value
*weight_sum += importance_weight * ranking_scale*
Normalise weight_sum to [0,1] range
Return normalised weight

Algorithm 6.2: Adaptive User Privacy Preference Modeling

Input: user_data (90-day dataset), privacy_thresholds
Output: Privacy Profile
Initialise user_profile =
For each data_type in user_data:
Calculate base_sensitivity = get_sensitivity_score(data_type)
For each role in roles:
Calculate role_weight = get_role_weight(role)
Apply time_decay = calculate_decay(current_time)
Generate preference_score = combine_factors(base_sensitivity, role_weight, time_decay)
Store in user_profile[data_type] = preference_score
Return user_profile

D6(vi-3):Key Findings and Implications

Table D(vi-4): summarises the key findings from the simulated scenario analysis, highlighting model robustness, adaptive capability, and performance validation. The analysis validated the privacy-aware framework's effectiveness in balancing robust privacy protection with efficient system performance. The implementation demonstrated strong performance metrics across different scenarios while maintaining appropriate privacy levels across various data types and usage contexts.

Table D(vi-4): Summary of User Experience Findings from Scenario Analysis

Key Findings	Details
Model Robustness	Successfully handled varying privacy requirements
	Maintained performance under different conditions
	Demonstrated consistent behavior across scenarios
Adaptive Capability	Effectively adjusted privacy scores based on context
	Showed appropriate sensitivity to preferences
	Maintained privacy-usability balance
Performance Validation	Confirmed real-world applicability
	Validated negotiation mechanisms
	Identified optimal operating parameters

This systematic evaluation confirms the framework's success in enabling dynamic privacy management while maintaining high user satisfaction levels, with processing times remaining efficient even under challenging conditions.

D6(vii) Role-Based Access Control Performance Analysis

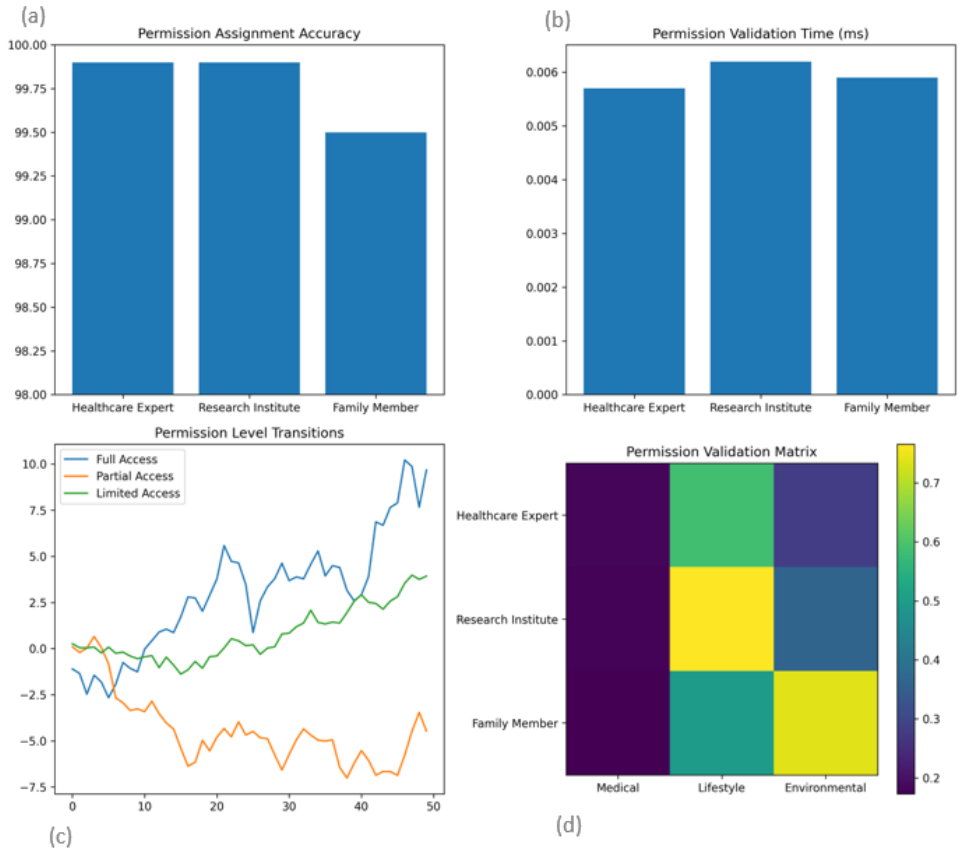


Figure D6(vii): Role-Based Access Control Performance Analysis showing (a) permission assignment accuracy, (b) validation response times, (c) permission level transitions over time, and (d) data type access validation matrix across stakeholder roles.

Appendix E: Artefacts in Chapter 7 ML-Driven Privacy Preservation & System Optimisation

E1: Data Processing Documentation

Code Snippets: GitHub repository.

i) Data documentation

Utilisation of datasets on IoT device logs, user consent data, electronic health records, anomaly data, and system performance logs for privacy scoring model:

1. IoT Device Logs (iot_device_logs.csv)

- **Purpose:** Analyse logs to identify data access patterns, frequency of access, device types, and timestamps.
- **Actions:**
  - Extract features such as access frequency, device types, and timestamps.
  - Identify unusual access patterns that might indicate potential privacy risks.
  - Analyse log timestamps for data access trends and irregularities.

2. System Performance Logs (system_performance_logs.csv)

- **Purpose:** Evaluate system stability, response times, and potential privacy-impacting anomalies.
- **Actions:**
  - Assess metrics like response time, CPU usage, memory consumption.
  - Identify correlations between system slowdowns and potential data breaches.
  - Analyse resource utilisation trends to detect privacy-related inefficiencies.

3. Anomaly Data (anomaly_data.csv)

- **Purpose:** Detect suspicious behavior patterns that could indicate privacy violations.
- **Actions:**
  - Utilise anomaly detection techniques (e.g., Isolation Forest, Autoencoders).
  - Compare detected anomalies with IoT device logs for cross-validation.
  - Use clustering techniques to group similar anomalies for better understanding.

4. EHR (Electronic Health Record) Data (ehr_data.csv)

- **Purpose:** Assess the sensitivity of stored health records and their access patterns.
- **Actions:**
  - Classify data based on sensitivity levels (e.g., high, medium, low).
  - Track user access permissions against the actual access logs.
  - Determine how often specific health records are accessed and by whom.

5. User Consent Data (user_consent_data.csv)

- **Purpose:** Ensure compliance with user privacy preferences.
- **Actions:**
  - Match consent preferences against EHR data access logs.
  - Identify instances of consent violations.
  - Quantify the number of times data was accessed beyond the agreed terms.

(ii) Key Machine Learning Tasks Performed

1. **Privacy Risk Prediction:**
    - Train an ML model to predict privacy scores based on features such as access frequency, consent compliance, and anomaly detection results.
2. **Anomaly Detection:**
    - Implement unsupervised learning models to detect irregular access patterns in IoT and system logs.
3. **Consent Compliance Analysis:**
    - Use classification algorithms to assess whether data accesses comply with user consent preferences.
4. **Data Sensitivity Scoring:**
    - Apply regression or clustering models to classify data sensitivity levels based on historical access patterns.
5. **Feature Engineering:**
    - Derive meaningful features such as:
        - **Time-based metrics** (access peaks, frequency analysis).
        - **User behavior profiling** (comparison of past and current behavior).
        - **Anomaly correlations** (linking system performance issues with privacy concerns).

(iii) ML model implementation steps:

1. **Preprocessing:** Clean and preprocess the datasets (e.g., handle missing values, normalise numerical features).
2. **Feature Engineering:** Extract relevant features for model training.
3. **Model Selection:** Choose appropriate ML algorithms such as Random Forest, XGBoost, or Neural Networks.
4. **Evaluation:** Use metrics like accuracy, precision, recall, and F1-score to assess the model's effectiveness.
5. **Privacy Score Calculation:** Combine the findings from all datasets to generate a comprehensive privacy score.

E2: Feature Importance and Contribution to Privacy Risk Prediction (Section 7.2.2.3)

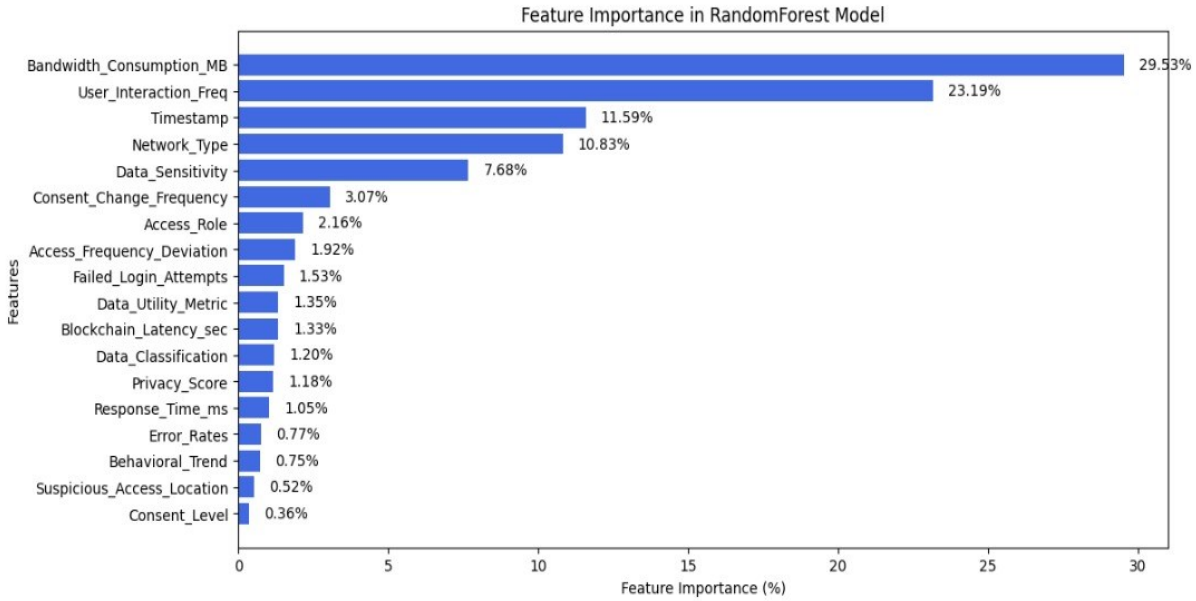


Figure E2(i): Feature Importance Before Ensemble Technique

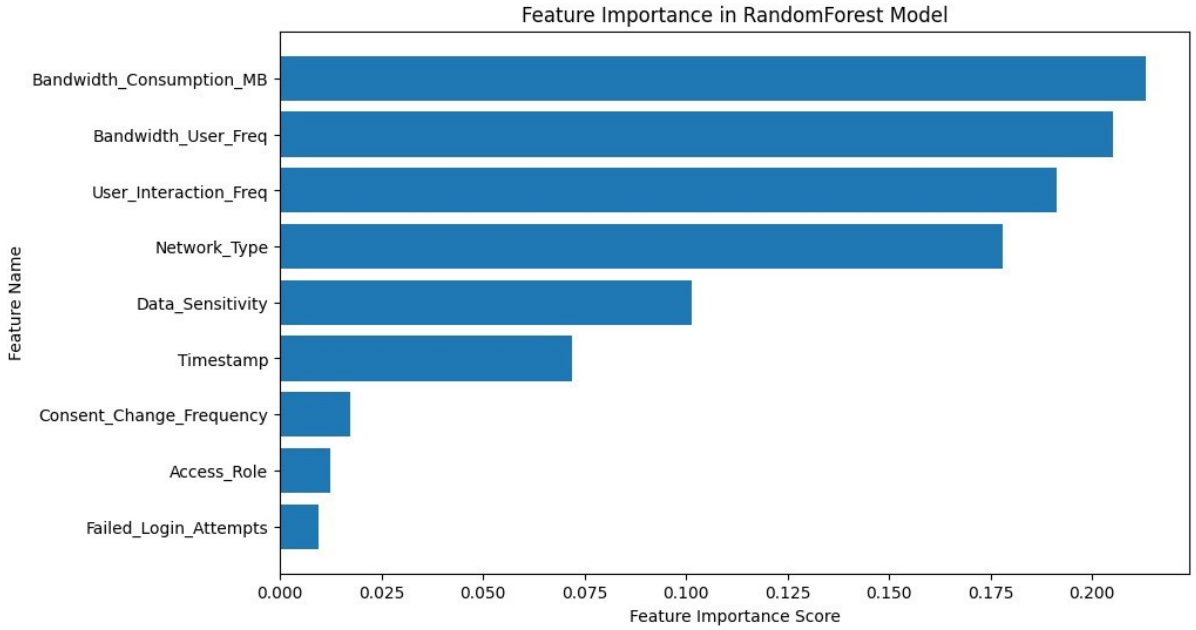


Figure E2(ii): Feature Importance For Prominent Features For Ensemble Technique

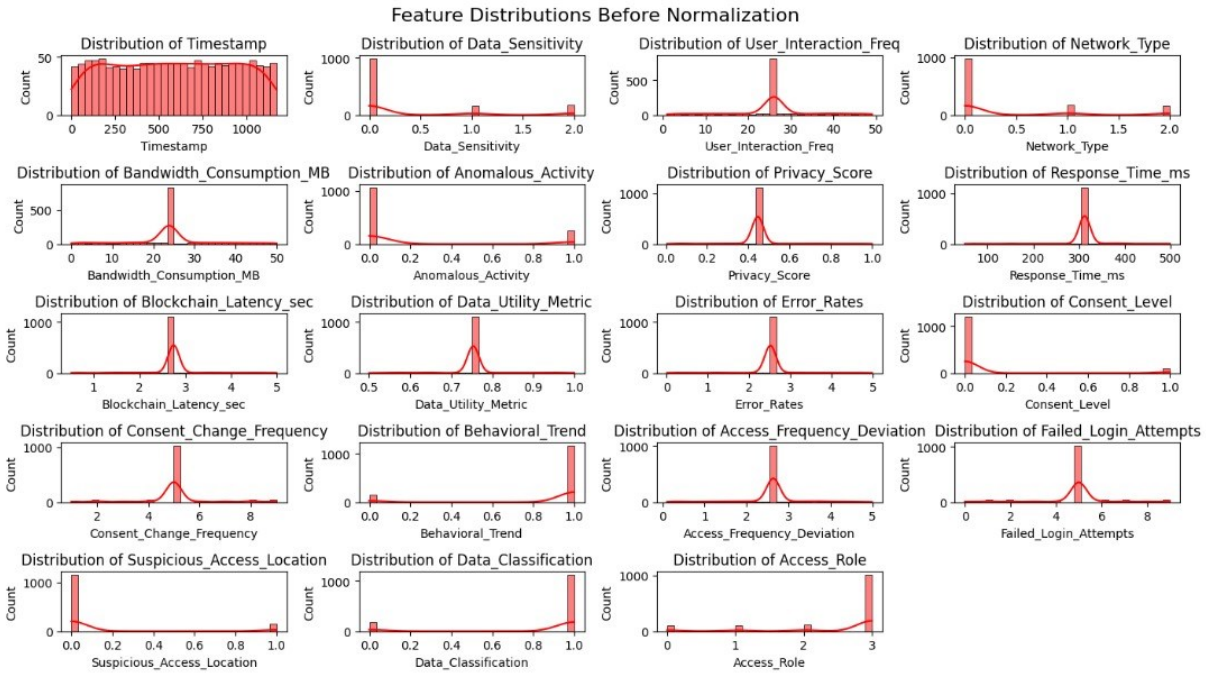


Figure E2(iii): Feature Distribution Before Normalisation

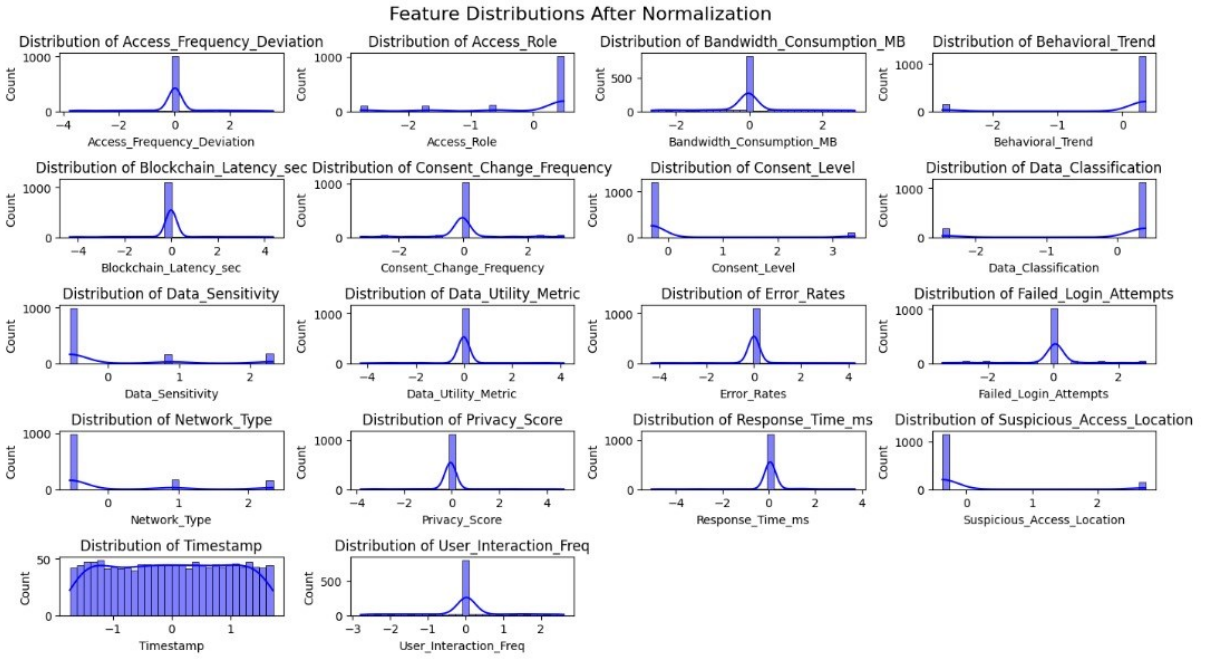


Figure E2(iv): Feature Distribution After Normalisation

The IDE environment for the Ensemble-ML algorithm is here

Sheffield Hallam University

OLUSOGO POPOOLA [redacted]

Converis - Ethics Review - Approval

converis@shu.ac.uk <converis@shu.ac.uk> 27 May 2021 at 16:25
To: "Popoola, Olusogo" <Olusogo.J.Popoola@student.shu.ac.uk>

Status change comment
DO NOT WRITE ANYTHING IN THIS NOTES BOX AS IT CAN BE SEEN BY ALL OTHER USERS. Proceed to select the workflow status and click Done.

- Dear Olusogo

Title of Ethics Review: Internet of Things (IoT) Security and Ethics
Ethic Review ID: ER32613049

The University has reviewed your ethics application named above and can confirm that the project has been approved.

You are expected to deliver the project in accordance with the University's research ethics and integrity policies and procedureshttps://www.shu.ac.uk/research/ethics-integrity-and-practice.

As the Principal Investigator you are responsible for monitoring the project on an ongoing basis and ensuring that the approved documentation is used. The project may be audited by the University during or after its lifetime.

Should any changes to the delivery of the project be required, you are required to submit an amendment for review.

Wishing you success you with your study

Kind regards,
Ethics Research Support

*** This is an automatically generated email, please do not reply ***