

A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions

POPOOLA, Olusogo, RODRIGUES, Marcos <<http://orcid.org/0000-0002-6083-1303>>, MARCHANG, Jims <<http://orcid.org/0000-0002-3700-6671>>, SHENFIELD, Alex <<http://orcid.org/0000-0002-2931-8077>>, IKPEHAI, Augustine and POPOOLA, Jumoke

Available from Sheffield Hallam University Research Archive (SHURA) at:
<https://shura.shu.ac.uk/32884/>

This document is the Accepted Version [AM]

Citation:

POPOOLA, Olusogo, RODRIGUES, Marcos, MARCHANG, Jims, SHENFIELD, Alex, IKPEHAI, Augustine and POPOOLA, Jumoke (2024). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions. *Blockchain: Research and Applications*, 5 (2): 100178. [Article]

Copyright and re-use policy

See <http://shura.shu.ac.uk/information.html>

A Critical Literature Review of Security and Privacy in Smart Home Healthcare Schemes Adopting IoT & Blockchain: *Problems, Challenges and Solutions*

Olusogo Popoola ^{a*} Marcos Rodrigues ^b Jims Marchang ^a Alex Shenfield ^b
Augustine Ikpehia ^b Jumoke Popoola ^a

^aDepartment of Computing, Sheffield Hallam University, UK;

Email address: o.popoola@shu.ac.uk

^bDepartment of Engineering and Math, Sheffield Hallam University, UK.

Abstract

Protecting private data in smart homes, a popular Internet-of-Things (IoT) application, remains a significant data security and privacy challenge due to the large-scale development and distributed nature of IoT networks. Recently, smart healthcare has leveraged smart home systems, thereby compounding security concerns in terms of the confidentiality of sensitive and private data and by extension the privacy of the data owner. However, PoA-based Blockchain DLT has emerged as a promising solution for protecting private data from indiscriminate use and thereby preserving the privacy of individuals residing in IoT-enabled smart homes. This review elicits some concerns, issues, and problems that have hindered the adoption of blockchain and IoT (BCoT) in some domains and suggests requisite solutions using the aging-in-place scenario. Implementation issues with BCoT were examined as well as the combined challenges BCoT can pose when utilised for security gains. The study discusses recent findings, opportunities, and barriers, and provide recommendations that could facilitate the continuous growth of blockchain application in healthcare. Lastly, the study then explored the potential of using a PoA-based permission blockchain with an applicable consent-based privacy model for decision-making in the information disclosure process, including the use of publisher-subscriber contracts for fine-grained access control to ensure secure data processing and sharing, as well as ethical trust in personal information disclosure, as a solution direction. The proposed authorisation framework could guarantee data ownership, conditional access management, scalable and tamper-proof data storage, and a more resilient system against threat models such as interception and insider attacks.

Keywords: IoT, smart home healthcare, PoA-based permissioned blockchain, authorisation framework, fine-grained access control, interception, privacy model, consent

1. Introduction

The application of the Internet of Things (IoT) in Smart Homes (SH) presents a significant challenge in terms of data security and user privacy, owing to the vast scale and distributed nature of IoT networks. IoT-enabled homes i.e., SH, comprising a network of uniquely identifiable connected devices, are capable of automatically acquiring implicit data [1]. Such data include sensor data from IoT devices in the environment surrounding the homeowner, data obtained through applications installed in mobile devices, or information gleaned from server log files that register the details of the network interactions between the homeowner and controller services (e.g., IP addresses). These IoT systems are capable of auto-organizing, sharing data and resources, and acting and reacting to environmental changes, with or without human intervention. IoT deployment in smart homes is increasing levels of comfort and convenience in daily living. For instance, IoT-enabled homes are integrable with digital healthcare facilities to benefit from smart healthcare using edge devices such as tablet PCs or PDAs installed with well-being monitoring applications, and in some cases, wearable technologies are installed to collect and share physiological data from home occupants in a transformative manner e.g., aging-in-place (Fig. 1). This approach often enables continuous healthcare to individuals by linking the home to mobile, and in-clinic health monitoring [2]. Sensing devices could be utilised in medical healthcare IoT-CPS to collect patients' routine health and physiological [3, 4] information classified as private [5]. However, the Internet of Health Things (IoHT) has emerged and leveraged the real-time access protocols of the Internet to provide comfort in well-being monitoring while also posing security challenges in data confidentiality and in preserving patient privacy [6].

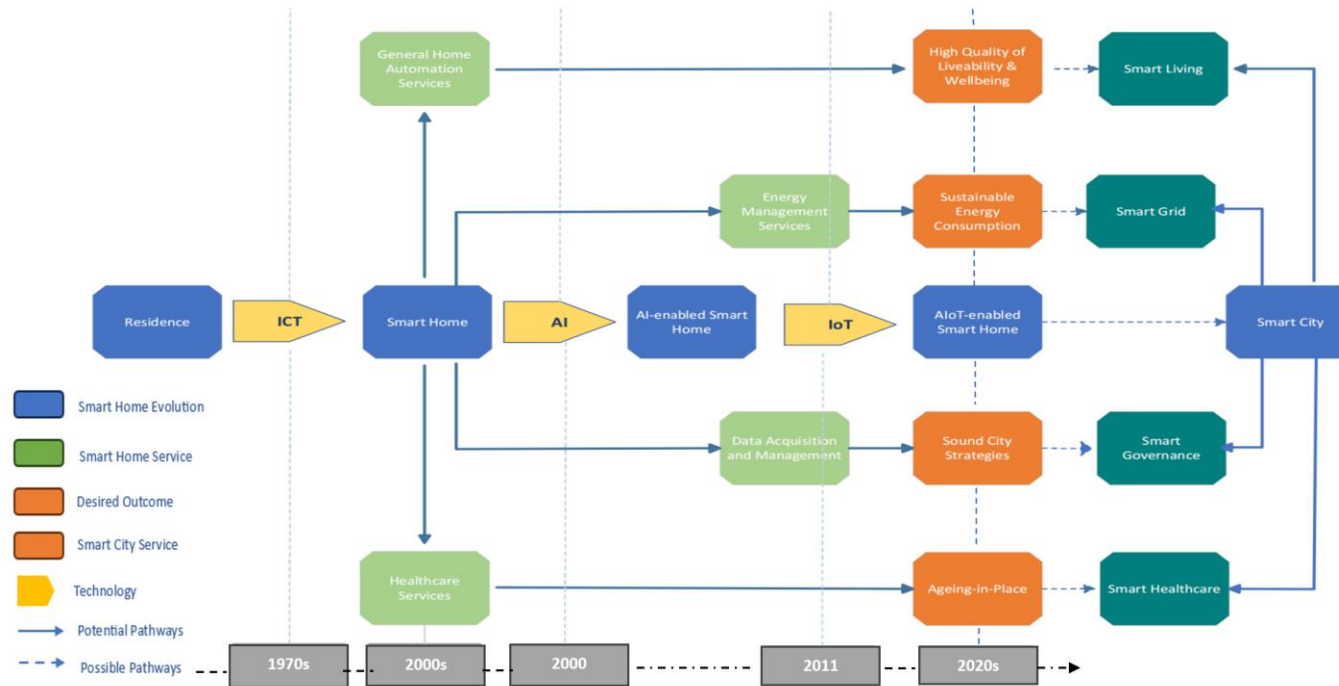


Fig. 1. Evolution pathway of smart home concept, related technologies, and services [7].

Challenges faced in smart healthcare include those of compromised devices, unauthorized access to personally identifiable information (PII), and the inability of homeowners to selectively disclose their information, thereby leading to concerns of indiscriminate exposure of sensitive and contextual information. The heterogeneous environment of IoT systems contributes to security and privacy challenges encountered in SH systems [8, 9]. The value chain of data management, consisting of data acquisition or collection, processing, storage, and usage, requires privacy protection using enabling technologies, as these present target surfaces, susceptible to attacks. The increasing number of internet-dependent devices in smart homes has led to a rise in privacy threats and attacks [10]. Such attacks can reveal sensitive information about homeowners, compromising their lifestyle and well-being. As privacy norms dictate, users should have control over their data, rather than complete withdrawal or non-disclosure. Users should be able to selectively disclose information and exercise control over who sees it. While privacy infringement can sometimes be acceptable when the eventual disclosure of the information is beneficial to the data owner e.g., in smart healthcare services where the data of monitored persons in smart homes collected using medical sensors are revealed to an eHealth expert systems to ensure their safety and well-being [11] [12] [13] [14] [15, 16] [11-16]. Moreover, intangible benefits of ethical disclosure of personal information for medical research, therapy logistics and design, marketing purposes, etc., could be supervised and controlled based on informed consent and acceptance [17], and the tenure of use as agreed by data owners [18, 19]. The increasing number of IoT devices in smart homes, such as wearables and nearables, has led to growing concerns over privacy and security risks. More so, when smart things are getting smarter and more vulnerable due to their small form factor and resource constraints which made conventional intrusion detection and protection schemes applicable directly to them. Moreover, in the health realm, where complex data are used to produce values that enhance human health, it has been established that standard strategies for addressing health data privacy problems are insufficient for protecting users' privacy. To lay some emphasis on user privacy and confidentiality of data, sensitive and private data will be defined and used interchangeably in the smart home healthcare scenario being discussed regarding personally identifiable information and their ethical disclosure.

The definition of sensitive and private data associated with ethical disclosure being discussed is as follows:

The terms "sensitive data" and "private data" are often used interchangeably, but there can be subtle differences, especially in the context of data privacy regulations, cybersecurity, and ethical standards. In the context of smart home well-being monitoring (Fig. 2), both terms are highly relevant, and understanding their implications is crucial for data management, protection, and compliance with legal standards.

- Private Data: "Private data" refers to information that is meant to be kept confidential within a defined group or setting. In a smart home context, this could be any data collected by smart devices that the user or household members would not want to share with the wider public. This can include general information like personal preferences in music or room temperature, schedules, or even shopping lists.
- Sensitive Data: "Sensitive data" is generally a subset of private data but refers specifically to information that, if disclosed, could potentially cause harm or pose a risk to the security or rights of an individual. Sensitive data often includes information related to health, racial or ethnic origin, political opinions, religious beliefs, or sexual orientation, among others.

In the realm of smart home well-being monitoring, sensitive data might refer to detailed health data, like information about an individual's chronic conditions, mental health, medication schedules, or biometric data (e.g., heart rates, blood pressure, sleep patterns). In smart home well-being monitoring, systems often collect a vast amount of data, some of which are intensely personal and potentially sensitive. For example:

- Biometric data collected by health monitors could be considered both private and sensitive, as unauthorized access could not only violate privacy but also potentially lead to identity theft or health insurance fraud.
- Information on an individual's daily routines or living habits could be private data, as it's information that the resident wouldn't want to be shared publicly but isn't necessarily sensitive, as it might not pose a direct risk if disclosed.

Given the potential overlap and differences, companies behind the design and deployment of smart home devices are yet to employ strict data security measures and follow relevant regulations (like GDPR in Europe, HIPAA in the USA for health-related information, or other local data protection laws) to ensure that both private and sensitive information is adequately protected against unauthorized access, disclosure, or other forms of data breaches. Furthermore, the management of such data should be transparent to the user, providing clear options for consent, and the ability to control what data is shared and with whom, ensuring the ethical handling of personal and sensitive information. Full compliance with these regulations requires privacy by design or other means of supporting the user of IoT devices [14] to secure their valuable personal information.

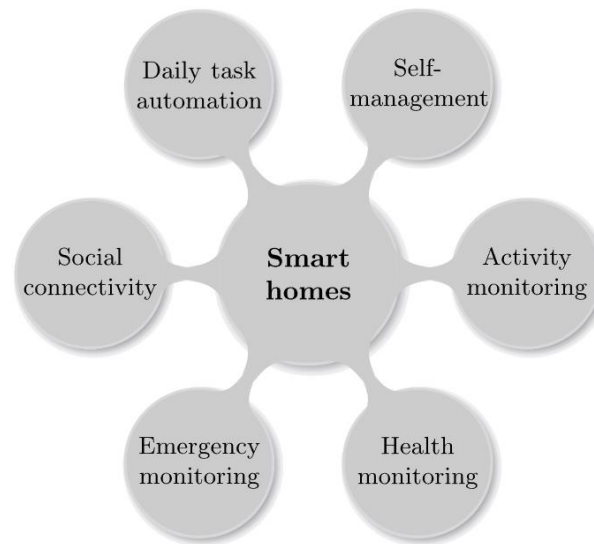


Fig. 2. Functionalities of a smart home healthcare scenario applicable for monitoring the elderly [11].

1.1. Strategies for IoT Data Protection

The IoT Core: A fundamental software component or service used in an IoT (Internet of Things) environment is referred to as the IoT Core. Sometimes refers to specific products or services, but the general idea is that an IoT Core is central to connecting, managing, and securing the multitude of devices in an IoT system. As a central engine, it connects and controls devices, with tenets such as security emphasised as an important characteristic, ensuring the deployment environment is secure (Fig. 3). The "core" in these services generally refers to the essential capabilities they provide in the context of IoT systems such as:

- Connectivity and control services: These are features that allow IoT devices to connect to the Internet or other networks and be managed remotely.
- Security: This is crucial, as IoT devices can be vulnerable to hacking and other security threats. The IoT Core often provides features to ensure secure device connections and data transfers.
- Data processing and integration: IoT devices generate vast amounts of data, which need to be processed, analyzed, and potentially integrated with other systems or databases.
- Device monitoring and management: This includes the ability to monitor the status of devices, update their firmware or software, and troubleshoot issues remotely.

"IoT Core" services are fundamental components in IoT architectures, providing the necessary infrastructure to connect, manage, secure, and integrate IoT devices at scale. Table 1 illustrates the need to secure the complex software/hardware that supplies IoT functionalities. The tenets can be applied to the processing of private and sensitive data in the smart home healthcare ecosystem such as personal and well-being data collected are given the required protection to avoid non-transparency of usage.

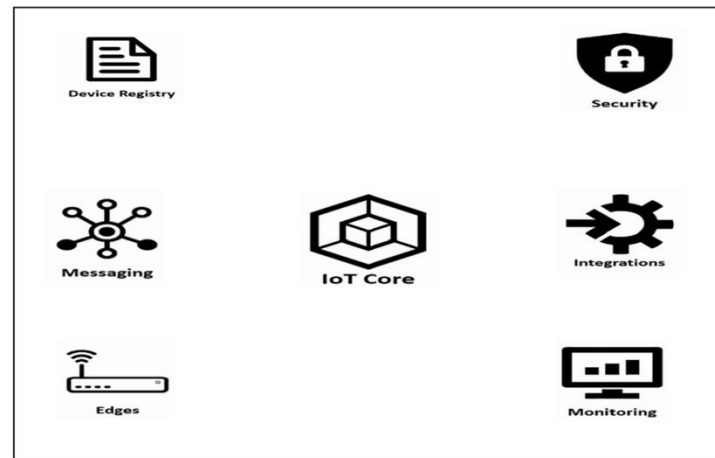


Fig. 3. Inside an IoT Core.

Table 1

IoT Core description.

Component	Description
Device Registry	Device registry of what is connecting to the user and how to identify those devices. This is stored in a table.
Security	Most importantly about how to ensure the device is allowed to connect to the user and that the device is communicating according to protocol i.e., prevent authorised disclosure of information.

Messaging	Messaging, at the heart, illustrates the transmission of messages back and forth (full duplex) to these devices. Requires having a very scalable and efficient Message Broker in the heart of the IoT Core.
Integrations	The need for simple integrations into other services outside of the core. These are things that the clouds provide such as integrations into databases, AI engines, into enterprise systems; or at the edge, integrations are needed into SCADA equipment, MES equipment, etc.
Edges	The edge concept has now been built in IoT Core. The ability to orchestrate these edges requires working with them to move processing between edge and core.
Monitoring	The need to be able to monitor the performance of the core, monitor the performance of devices, and monitor the overall health of how the system operates.

Blockchain Technology (BCT): Blockchain is a type of distributed ledger technology (DLT), and this technology relies on distributed technology with built-in confidence mechanisms to ensure data integrity to share both data and business processes. Certainly, blockchain is now introducing a new evolutionary cycle to database management development and it can be adopted as a solution for the ethical disclosure of personal data in a smart home healthcare setting. Blockchain is more than just a database that stores and verifies transaction data. Although blockchain was originally conceived to address gaps in the current architecture of financial systems, these limitations affect identities, currencies, and contracts. Likewise, blockchain architecture is also designed for security. Its security features include the immutability and fault tolerance of the database ledger, and the public key infrastructure (PKI) which secures the digital assets of individual blockchain users. Nevertheless, there have already been some high-profile hacks of blockchain systems, and newer blockchain networks are implementing creative ways to mitigate ongoing risks. Research efforts on addressing associated risks will be discussed extensively in the later section of this study. However, the adoption of blockchain application is on the increase as shown in Fig. 4, and several consensus algorithms (Fig. 5) has evolved from the traditional PoW to fit into the security demand of domains that require blockchain to benefit from its tenets of CIA.

Evolution	Products
1 st Generation	Currencies <ul style="list-style-type: none"> • Bitcoin • Bitcoin like
2 nd Generation	Contracts <ul style="list-style-type: none"> • Financial Services • Crowdfunding • Prediction Markets • Smart Property • Development platforms • DApps
3 rd Generation	Digital Services <ul style="list-style-type: none"> • DNS • Digital Identity
4 th Generation	Digital Infrastructure <ul style="list-style-type: none"> • Government • Education • Health • Publishing

Fig. 4. Evolution of Blockchain.











PROOF OF WORK (PoW) <ul style="list-style-type: none"> • PoW allow miners to add a new block to the network based on the computation done to find the correct block hash. 	
PROOF OF STAKE (PoS) <ul style="list-style-type: none"> • PoS uses a staking mechanism where participants lock up some of their coins to get selected for block addition. 	
DELEGATED PROOF OF STAKE (DPoS) <ul style="list-style-type: none"> • In DPoS mechanism, the block delegate's selection is based on voting. It is an additional layer to PoS. 	
BYZANTINE FAULT TOLERANCE (BFT) <ul style="list-style-type: none"> • BFT works on the system to stay intact even if one of the nodes fails with constant communication among nodes. 	
PROOF OF AUTHORITY (PoA) <ul style="list-style-type: none"> • Proof of Authority relies on the validator's reputation to make the blockchain work properly. 	
PROOF OF IMPORTANCE (PoI) <ul style="list-style-type: none"> • PoI rewards user with importance scores which eventually help them to become block harvesters. 	
PROOF OF CAPACITY (PoC) <ul style="list-style-type: none"> • PoC uses the storage capacity for mining a block in a decentralised network. 	
PROOF OF ACTIVITY (PoA) <ul style="list-style-type: none"> • Proof of Activity combines the capabilities of PoW and PoS algorithms. 	
PROOF OF BURN (PoB) <ul style="list-style-type: none"> • PoB allows miners to add their block by sending some of their coins to an unspendable account 	
PROOF OF ELASPE TIME (PoET) <ul style="list-style-type: none"> • PoET uses a lottery time-based consensus algorithm, distributing wait time to each participating node. 	

Fig. 5. Some Consensus Algorithms in BCT [21].

Permissioned blockchain implementation presents a viable solution due to blockchain's internal mechanisms which are designed to ensure data security and provide privacy through cryptography and consensus algorithms. These built-in mechanisms convert data transactions into hashes to compose blocks. Such blocks follow each other sequentially in what can be described as a chain. This architecture is supported by cryptography and ensures the integrity of the ledger. Although nodes in a permissioned blockchain hardly trust each other, their identities are authenticated, allowing the system to apply more efficient protocols for withstanding Byzantine failure than in a permissionless blockchain. A combination of lightweight cryptographic algorithms and secured privacy techniques has been a key enabler in the development of blockchain and its emerging applications. Hence, issues of data privacy are progressively being tackled in blockchain, providing data confidentiality and immutability, and making the desirable security attribute in private BCT duly applicable in the health sector [22] [23] [24] [25] [22 -25].

This current study discusses the evolution of blockchain beyond virtual currencies where other technologies such as smart contract management, NFTs, and the digitization of commercial and organizational registries have been integrated. Smart contracts can be written on the blockchain and executed by all nodes on the block. Table 2 illustrates the different categories of blockchains, with differences in their Speed of Consensus, Trusted Authority, and the number of TAs required. All categories of blockchain (BC) share common properties such as the usage of a decentralized P2P network for transactions, digital signature requirements, and reliance on consensus to sync the replicated distributed ledger of transactions across the blockchain network (BCN).

Table 2
Blockchain Classification.

Types	Description	No. of TA	SoC	Scenario
Private Blockchain	Write privileges under the control of an organisation	1	Fast	Information management and sharing within an organisation
Public Blockchain	Anyone can be a participant and it is accessible globally	0	Slow	Global decentralized scenarios
Consortium Blockchain	Controlled by pre-selected nodes within the consortium	\geq	Slightly Fast	Businesses among a selected organisation

A useful advantage of a permissioned blockchain is the possibility of implementing it as both a private-permissioned blockchain where it presents high scalability and a public-permissioned blockchain in which medium scalability is achievable as against low scalability in the public permissionless blockchain (Fig 6).

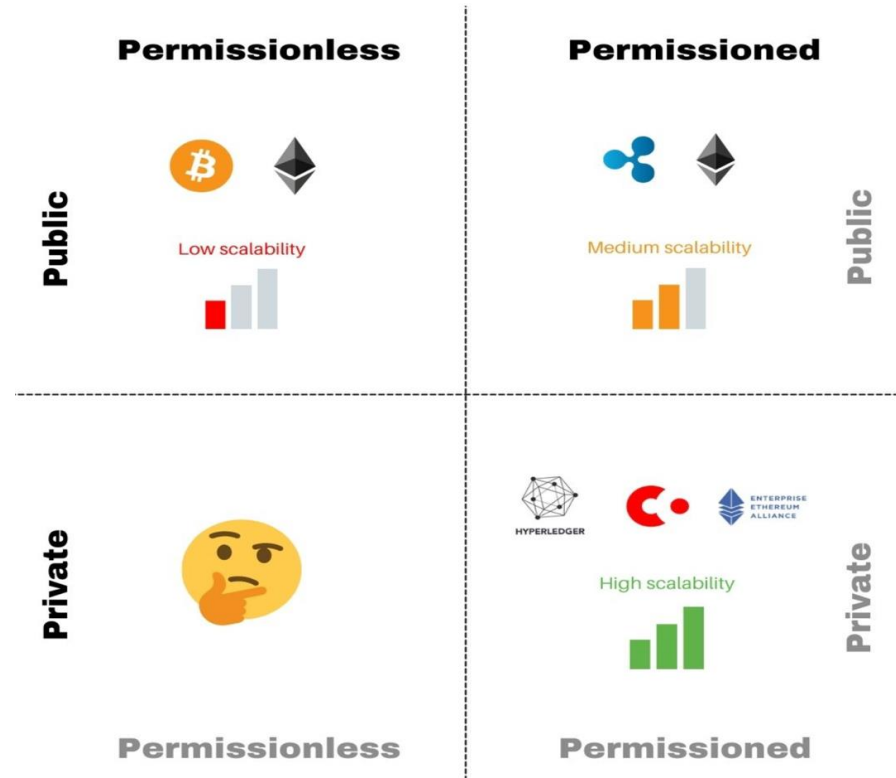


Fig. 6 Blockchain type matrix [26].

This review therefore suggests a combination of IoT security techniques and permissioned blockchain to propose a permissioned BCoT authorization framework, emphasizing secure data exchange and distribution among IoTs and computing nodes. Hybrid cryptography techniques are utilised to ensure privacy preservation, a potential solution to indiscriminate disclosure of private data in smart home healthcare delivery. An overview of blockchain categories and development ecosystem is further illustrated in Fig. 7 and explained in Table 3. The permissioned approach is beneficial due to increased privacy control, higher transaction rates, scalability, and little or no gas cost requirement, although there are arguments on the counter-intuitiveness of private and permissioned blockchain to the goal of decentralization [27]. Blockchain is built on asymmetric key encryption, hash values, Merkle Tree, and P2P networks. Thus, blockchain allows decentralized transactions to take place and acts as an unchangeable record. Recently, BCT has emerged as a potential solution for secure, trusted, efficient storage, and data sharing [28]. The long-term factor supporting the excellent fit of blockchain and IoT integration in the smart healthcare realm [29] is the decentralised

nature and distributed network of the technology. However, the computational intensity and high energy consumption of traditional consensus mechanisms in BC-based systems in securing data processes e.g., Bitcoin, uses 707 kilowatt-hours per transaction [30] makes it unsustainable nor scalable.

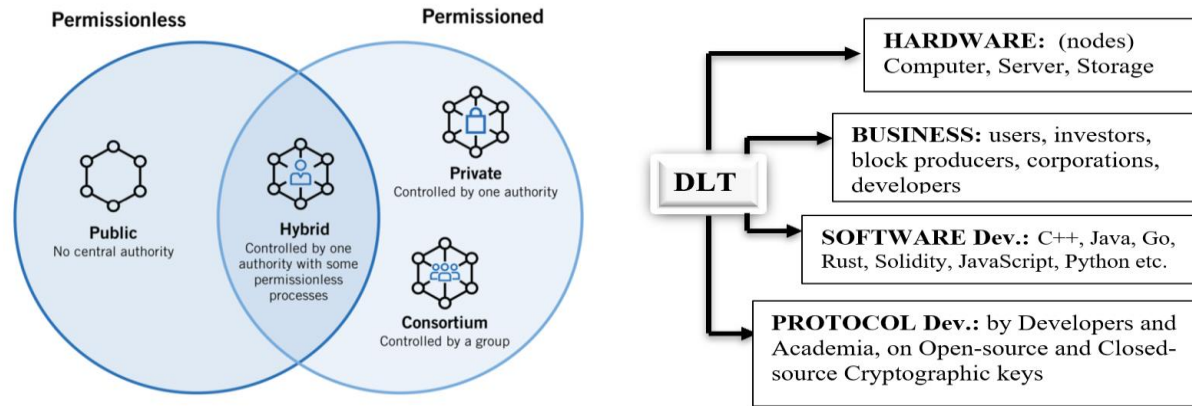


Fig. 7. Overview of DLT Structures and Aspects of DLT Ecosystem as adapted [31].

Table 3

Comparison between Permission and Permissionless BCNs.

Permissioned	Permissionless
Permission is required before participation	Anyone can participate
Participants are well-known to others	Participants not known
The number of participants is limited	Unlimited number of participants
Data security is offered	Offers less data privacy
Instant consensus predictability	Weak consensus inevitability
Transaction rate is high (good throughput)	Transaction rate is low (low throughput)
Highly scalable	Scalable
Vulnerable to participant's collusion	Vulnerable to 51% attack
Enable finality of data	No finality of data (51% attack)

1.2. BC-Enabled IoT

A framework that integrates data management in IoT devices with a lightweight blockchain implementation using the Proof-of-Authority (PoA) consensus mechanism is considered in this paper. PoA algorithm provides a considerably low computational, latency, and energy overhead during the data secure process, and is suitable for resource-constrained IoT devices. Moreover, the introduced framework offers higher security levels since distributed networks rarely suffer from a single point of failure, while asymmetric cryptography disallows unauthorized access aimed toward data fabrication, modification, and manipulation. Furthermore, the structure supports access management, device binding, fine-grained access control, and data ownership. Implementation of a Smart Contract adds another level of control that maintains rules, authentication, and communication between the participating nodes of the system design. Earlier studies suggest that PoA can handle SH communications at high transaction rates with validation performed by randomly selected trustworthy, non-high-performing, inexpensive nodes, thereby eliminating earlier energy-hungry, computationally intensive Proof-of-Work and share-based Proof-of-Stake [32]. The proposed framework provides an ethical data access approval that is acceptable to all participating nodes, where access request to the IoT devices within home network components is considered the basic element of permissibility that could prevent data leakage and uphold the privacy of individuals under observation.

The connection of smart devices through blockchain enables distributed devices to act autonomously as these devices generate enormous amounts of dynamic and unstructured data, and these data being IoT's true value need to be protected. Hence, BCT can potentially douse security concerns of lack of data usage transparency, traceability, and reliability posed by IoT data collection processes in smart home systems. Authors in [33] mentioned the utilization of Hyperledger Fabric's chain code as an instance of smart contracts in permissioned BCNs where the majority of permissioned blockchains employ a deterministic consensus mechanism that can easily achieve fast consensus among the authenticated users [34]. Fig. 8 illustrates the layered implementation of a permissioned blockchain.

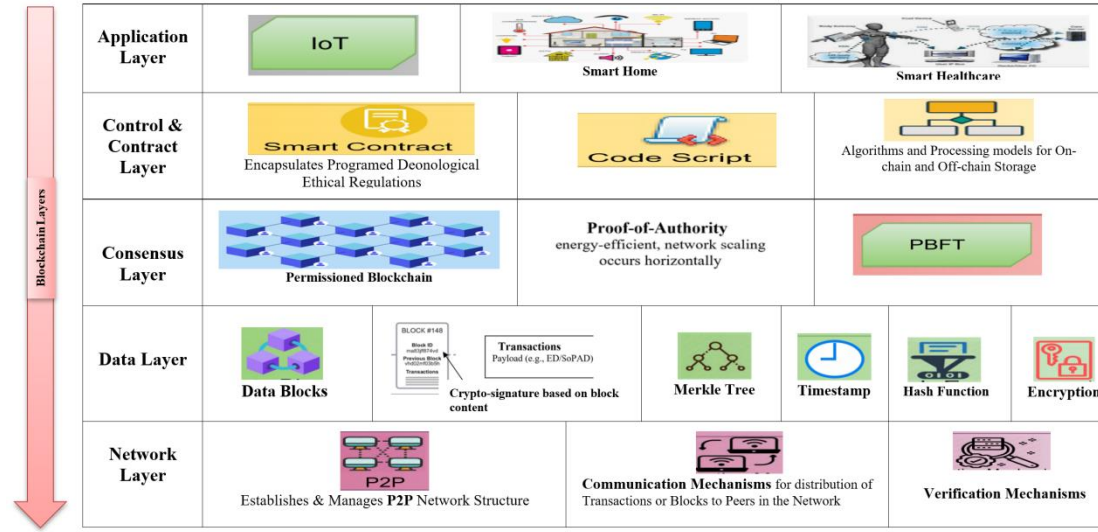


Fig. 8. Layered implementation in the proposed PoA-based Permissioned BC as adapted [19].

1.3. Authorisation Scheme through Permissioned Blockchain-enabled Smart Home Healthcare of Things

This review discussion is on an authorization framework and user-centric privacy control scheme based on smart contracts and permissioned blockchain. The goal is to prevent unauthorized data collection and disclosure while allowing users to specify their privacy preferences. The focus is on confidentiality, which is one of the three basic security requirements (CIA), that explores the use of blockchain as a viable DLT to ensure data immutability, transparency, traceability, and auditability. The proposed approach is not limited to smart home healthcare systems but applies to several IoT-enabled applications.

The proposed framework aims to apply blockchain technology to address data security challenges in smart home healthcare systems. The challenges include the lack of fine-grained access control and data ownership schemes, which often lead to credential stuffing and insider attacks [35, 36]. The framework proposes the use of a PoA-based permissioned blockchain and smart contracts assigned to each node for role-based access control and data management. The second challenge is the lack of data transparency and auditability, which can be mitigated through blockchain's ability to provide a transparent and auditable regime for data collection and storage in a private network. The main objective of the use of a permissioned blockchain is to establish transparency in the sharing of sensitive information such as medical records or behavioural data. However, this transparency should be balanced with privacy preservation, as the degree of information disclosed is directly proportional to the quality of care received. Therefore, a justifiable relationship must be established between blockchain features of data immutability, transparency, traceability, and privacy [37]. In a smart home healthcare system, the information disclosed is stored in both on-chain and off-chain locations, with details such as timestamp, degree of disclosure, authorised recipient, the purpose of sharing, and information content being recorded. The content of the information is often encrypted and can only be decrypted by the authorized recipient.

The implementation of permissioned blockchain can help to reveal cases of medical service denial, abuse, or negligence in healthcare delivery. Through the auditing processes, maltreatment, inappropriate behaviour, or lack of professionalism can be made transparent, as authorised network participants can monitor who gets what based on their role in the blockchain ecosystem. The immutability and traceability of data transactions in the blockchain also allow for the establishment of a reputation-based system, where each entity has a separate smart contract to regulate data sharing. Overall, transparency in permissioned blockchain must constantly be redefined in the context of privacy preservation, and the use of blockchain in healthcare should be accompanied by transparent and ethical use of behavioural, implicit, and physiological data.

The third challenge is the failure of the use of appropriate tamper-resistant data storage facilities. The traditional database management system (DBMS) is unable to protect against database breaches, data manipulation, and corruption due to the limited database operation for persistent storage the CRUD configuration (Create, Read, Update, and Delete) offers. Blockchain technology's immutability and append-only feature make it more secure through the implementation of the CRAB model [38] for persistent storage applications. The four basic operations of CRAB (Create, Retrieve, Append & Burn) are more efficient and better suited for data storage schemes with data privacy preservation motives. In smart home healthcare delivery, keeping private data in off-the-chain storage instead of on-the-chain is recommended for data scalability because blockchain data storage capability, by default, is limited. A permissioned or closed blockchain is also viable to complement the tamper-resistance property of blockchain data. The data ownership/provenance scheme applied makes it relatively easier to delete personal data based on an individual's request through a process called forking. Overall, exploiting blockchain characteristics of decentralization, immutability, and asset management is central to this solution delivery.

The use of both on-chain (blockchain) and off-chain (IPFS) storage can improve data flow management and scalability. Private and sensitive data can be stored in IPFS while only transaction-related data i.e., hashes of encrypted data is stored on-chain. This increases the number of transactions that can be accommodated within a block.

1.4. Motivation

Existing systems lack adequate access control for the disclosure of sensitive and private data. In most cases, the consent of the data owner is rarely considered, thereby making data ownership, sovereignty, and provenance barely attainable. For instance, a lack of fine-grained access control and data ownership schemes often lead to credential stuffing and insider attacks [35, 36]. Furthermore, discussions on integrable privacy models as a means of achieving privacy by design into most authorisation framework for ethical disclosure of private data in a smart home system without any introduction of noise [23] or undue randomness into data in transit has not gained sufficient attention. An authorisation framework that is best suited for resource-constrained IoT nodes and at the same time computational and energy efficient and underpins net zero initiatives is also desirable in the pervasiveness of IoT in the smart healthcare domain. This motivates the investigation of a new authorisation framework for ethical disclosure of private data in a smart home healthcare ecosystem using a combination of publisher-subscriber smart contracts and PoA-based permissioned blockchain as a service.

1.5. Contributions

The main contribution of this paper is how the combination of lightweight solutions e.g., transport encryption scheme for IoT, PoA-based blockchain, and specific smart contracts built on a consent-based privacy model (privacy by design) can play a crucial role in improving privacy preservation techniques in the smart healthcare, through their use as a recipe of an authorisation framework. The specific contribution of the research is as follows:

- Towards considering the several security issues such as data confidentiality, integrity, authentication, etc., and minimizing the associated computation and communication overheads in IoT-enabled smart homes for well-being monitoring, we examine the best fit hybrid transport encryption schemes of elliptic curve cryptography (ECC) and Advances Encryption Scheme (AES). This is based on a remote user mutual authentication scheme for the IoT environment that establishes authentication between home sensors and home gateway, as well as between the home gateway, IPFS, and eHealth monitoring nodes. This will also be the underlying encryption technique utilised in the blockchain.

This paper puts forward a consent-based privacy model, as a decision-making recipe for ethical disclosure of the homeowner's sensitive or private data during the continuum of care.

- A PoA-based permission blockchain is outlined in this paper as the underlying security provision for supervised transparency, traceability, immutability, and auditability of sensitive and private data emanating from the smart homeowner being monitored and placed on a care plan (continuum of care).

- A publisher-subscriber smart contract model is described in this paper for fine-grained access control to ensure disclosure of information that benefits the data owner, that is, the homeowner, and all information stakeholders in a transparent manner.

Lastly, the study discussed the extensive threat model evaluation for privacy preservation.

Using the approach of content analysis, this study highlights the growing interest in the academic community and identifies three key research areas:

(i) IoT and Blockchain implementation in smart home applications for data security gains.

(ii) IoT and Blockchain implementations for secure data storage and management of private data in smart home-based healthcare services.

(iii) IoT and Blockchain implementation for privacy preservation in digital healthcare systems (internal consortium/secure disclosure of transparent private data of the smart home user).

Another contribution of this survey is summarised as follows:

1) Discussion of the benefits and applications of integrative BCoT for smart healthcare.

2) Introduction of the conceptual authorisation framework from Blockchain-enabled IoT in (i) Smart home well-being monitoring (ii) data storage and management (i.e., electronic health record-EHR and medical health record-MHR management), and (iii) digital healthcare system analysis and diagnosis, where the Blockchain network can guarantee ethical disclosure of information that is beneficial to information stakeholders i.e., data subject/publishers and subscribers in the smart home healthcare ecosystem.

3) Highlighting the challenges and opportunities that require implementation in the digital healthcare domain by researchers.

1.6. Research Aim

This study aims to address security and privacy concerns in smart home healthcare systems by proposing an authorization framework using permissioned BCT. The research questions cover various aspects of data security and privacy, such as access control mechanisms, secure data storage, and threat evaluation. The

study aims to examine security threats to data privacy in smart homes, design a middleware for access control using BCT, and validate the system's performance. The potential impact of the study is significant, as it addresses the growing concern of IoT-based attacks on vulnerable groups [39, 40] and proposes a consensus-based transaction endorsement equipped with a privacy preservation model and data ownership to control selective disclosure of personally identifiable information. The proposed model could be applied across all smart home settings.

In this paper, the specific research question raised, examined, and proffered with solutions are:

RQ1 – How suitable are existing transport encryption techniques in tackling emerging interception threat models targeted towards depriving users of privacy due to unethical disclosure of personally identifiable information when resource-constrained IoT devices are used in the smart home healthcare delivery ecosystem?

RQ2 – How can a consent-based privacy model be implemented for decision-making in the ethical disclosure of sensitive or private data?

RQ3 - How can IoT, Blockchain technology, and smart contracts be exploited to design an authorisation framework for ethical disclosure of private data during the acquisition and transmission of data in smart home healthcare delivery processes that could improve users' privacy?

Considerations to include consent-based access control to safeguard against the illegitimate collection of private data; and the storage approach applicable to ensure secure storage of such data in a smart home healthcare ecosystem.

The direction to follow in proffering a solution to this problem is to control and protect:

- 1) The data acquisition, collection, monitoring, and sharing process,
- 2) The location(s) where and how the collected data is stored, and
- 3) To issue information to stakeholders with smart contracts for fine-grained access control to publish, subscribe, and use such data (i.e., nodes that can acquire, monitor, and store private data).

The questions above are further examined through a thematic analysis of related work. Each theme section provides research outcomes and areas that can be developed.

The potential impact of the research is as follows:

- The scenario of the elderly in a smart home is essential in a society with an aging population.
- Telemetry is a foremost preventive care method rendered over the air (remotely), attackers can take advantage of vulnerable IoT's and nodes.
installed across the P2P ecosystem if they are not secured.
- A consensus-based transaction endorsement will enable selective disclosure of data owner's (the elderly) information within the smart home healthcare ecosystem. In the absence of this purpose, there is most likely to be an abuse of information, whether deliberately or unintentionally.

1.7 Organisation

The remainder of the paper is structured as follows. Section 2 is a detailed literature review that explains the recent security and privacy challenges and outlines related work that adopts BCoT in smart home healthcare systems, including the current state of the art, focusing on their contributions compared with this

work. Discussion of viable solutions through a descriptive authorisation framework, privacy model, and evaluation procedures are presented in section 3. Finally, section 4 presents the conclusion, the paper's limitations, and possible future research.

2. Literature Review

The issue of data privacy and security in healthcare data sharing is a significant and concerning topic, particularly in the context of Machine-to-Machine data transfer protocols. Consequently, numerous reviews, research studies, and investigations have been conducted to address this problem and offer effective solutions in the healthcare domain. This research work tries to mitigate the persistent challenges and ensures the protection of sensitive healthcare data. In this section, some of the research papers written to address these issues in diverse domains including in healthcare will be surveyed and analyzed, extracting the findings made, the limitations experienced, the techniques employed, evaluation methodologies, and characteristics investigated in their respective research works.

2.1. Challenges and problems with smart home healthcare schemes and BCoT adoption

There are various risks associated with introducing blockchain technology to most domains. The following are the most encountered risks: strategic risk, information security risk, operational and IT risk, key management risk, data confidentiality, and security risk. Thus, different sectors should be prepared to encounter these risks and should implement a higher level of risk management [41]. However, types of risks in blockchain can be further categorised into three main risks, namely, standard risk, smart contract risk, and value transfer risk.

Health record maintenance and sharing are one of the essential tasks in the healthcare system. In this system, loss of confidentiality leads to a passive impact on the security of health records whereas loss of integrity leads can have a serious impact such as loss of a patient's life. Therefore, it is of prime importance to secure electronic health records. For instance, the health records are represented by Fast Healthcare Interoperability Resources standards and managed by Health Level Seven International Healthcare Standards Organization [41]. Centralized storage of health data is attractive to cyber-attacks and constant viewing of patient records is challenging. Therefore, it is necessary to design a system using efficient decentralised data management technologies that helps to ensure authentication and also provide integrity to health records.

Delivering health care to people has become revolutionized due to technological advancement such as seen in the smart home application where individuals live independently, are assisted, or aging in place with the help of embedded systems and medical devices; these emerging technologies are not without their challenges [42, 43, 44, 45, 46, 47, 48] [42-48]. The incorporation of different health sensors, handheld devices (PDAs), and Internet access to drive them, has proven to be of great potential for the significant improvement of the quality of service and experience in remote health care. Instances of IoT devices used in physiological sensing for monitoring vital and behavioural signs are emerging and constantly gaining popularity. For instance, the growth of the Body Sensor Networks (BSN), a network of sensors, wearables, nearables, and controllers in the smart home environment is attributed to the proliferation of IoTs. Smart home residents' or patients' health information constitutes the private data being transmitted over the air using BSN and stored in database servers. Therefore, in the presence of adversarial behaviour, the IoTs as data publishers, and storage facilities are potential attack surfaces and are all vulnerable to varying degrees of interception threats. In addition, security attacks on communication channels e.g., interception, or malware injection into software applications running sensing devices could compromise devices, grant unauthorised access to transparent data on the data publisher-subscriber network, allow indiscriminate collection or infusion of incorrect data to the data collection process (i.e., data modification or fabrication). Eventually, this can result in a wrong diagnosis, treatment, or unethical disclosure of personal data revealing the lifestyle and well-being of smart home healthcare system users. Therefore, an efficient data protection strategy fosters interoperability along the value chain of digital healthcare systems to reliably support the continuum of care in the smart home healthcare ecosystem.

A viable solution is the integration of IoTs data processing with the secure data storage possible with the use of BCT. However, the slow adoption of IoT and Blockchain integration (BCoT) in managing user privacy in the digital healthcare domain is due to several reasons which include strict guidelines on patient privacy rights as regards their consent on personal information sharing, resource constraints on the deployment of robust transport encryption on IoTs such as wearables, and limited information on the underlying techniques applicable for ascertaining privacy, classification of approach – private or public, and misconceptions on data management in BCT, making the combination of BCoT debatable as a solution to data security and privacy preservation in the smart healthcare sector.

Navigating the trade-off between openness and privacy of user information represents a significant obstacle to the adoption of permissionless blockchain for medical purposes. Although blockchain technology is not without its associated challenges, issues categorised in Fig. 9, are being investigated by the active research community on Blockchain adaptation, resulting in a gradual increase in the rate of adoption due to its potential widespread application domain. For example, there is an ongoing discussion on the possibility of implementing private permissionless blockchains [49]. It is argued that deploying a smart contract on a permissionless private network automatically creates a private (side) chain associated with that contract.

Moreover, the advantages, expansion, and use of Blockchain technology in healthcare applications have posed significant research challenges that necessitate further exploration.

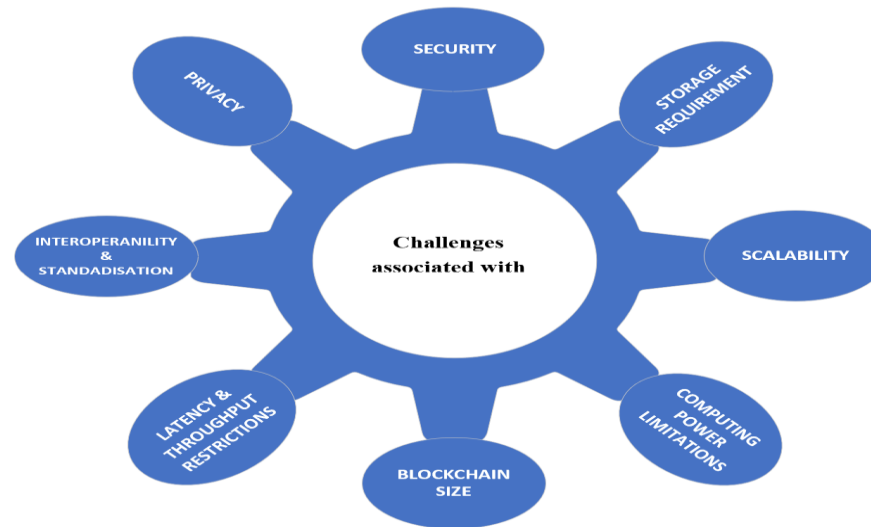


Fig. 9. Classification of problems associated with implementing Blockchain technology in healthcare applications.

Some recent challenges stem from the environment of open data and transparency observed in Blockchain. This contributes to emerging concerns that resulted in the slow adoption of BCT aside from the challenges with conventional consensus algorithms that are not energy efficient or eco-friendly. The benefits of blockchain classification i.e., with variants of permissionless, permissioned, and hybrid, are currently exploited to implement data security in many sectors including the healthcare domain. When properly implemented, Blockchain technology could be a useful solution to unauthorised information disclosure in digital healthcare applications and limitations that adversely affects data confidentiality, protection, sharing, usability, interoperability, and real-time medical data updates. The combination of Blockchain with AI, ML, and Federated learning for protecting personal data, authenticating IoT device information through transport encryption of sensitive medical data, secure data storage, etc., is a confirmation of the efficacy that Blockchain features can complement to achieve. In essence, an adequate procedure for the implementation of a lightweight authorisation framework, that is consent-centric and combines CIA (confidentiality, Integrity, and availability) security algorithms with access control mechanisms, that could guarantee ethical disclosure of private data, is also achievable with Blockchain technology. Summaries of recent related reviews that discussed challenges, opportunities, adoptions, and key contributions of Blockchain technology are illustrated in Tables 4 and 5.

This paper focuses on how blockchain is explored to achieve the transparency of data collection processes and monitor the purpose of the use of collected data to adequately preserve user's privacy. This involves integrating and optimising the architecture of IoT-enabled smart homes and blockchain specifically for healthcare-related applications, that is, in providing supervisory control on data acquisition, secure data access and storage, and digital healthcare monitoring systems). This paper discusses the pros and cons of blockchain-enabled smart home systems for well-being monitoring and healthcare delivery. The paper also classifies the technologies' potential applications under this domain and introduces a conceptual authorisation framework built on the synergy of IoT in smart homes, smart contracts, and blockchain applications to different domains in healthcare. In addition, a systematic analysis of previous papers published on blockchain-based intervention in the health-related domain is provided.

Table 4
Challenges and opportunities of BCT in the healthcare sector.

Direction of discussion	Highlight	Ref
Stakeholders Perception	On smart healthcare system stakeholder perspective.	[50] [51] [52] [53] [54] [55] [56]
Fit-for-purpose Approach	On data management, provenance, and security.	[57] [58] [59] [60] [61] [62] [63]
Trustworthiness	On trust, scalability, and governance.	[64] [65] [66]
Privacy and Authorisation	On confidentiality, system transparency, privacy-preservation, and secure data management and storage i.e., of EHR and EMR.	[67] [68] [69] [70] [64] [71] [72] [73] [66] [74] [75] [59] [76] [77]
Technology Integration	On ecosystem interoperability and resource constraints.	[78] [70] [79] [80] [81] [82, 83]
Remote Monitoring	On applications for observing patients securely.	[68] [69] [84] [71] [66]
Intelligent Sharing	On transactional data intelligence, data sharing, and mutual authentication.	[72] [69] [66] [79] [59] [85] [86]
Control Techniques	On data ownership and access control.	[66] [75]
Efficient Logistics	On drug tracking, secure pharmaco-logistic, integrity, and anti-counterfeiting.	[68] [87] [58] [71] [88]
Distributed Storage	On secure storage of data in a distributed environment.	[89] [66] [90] [91]

Table 5

Adoption of BCT in the healthcare sector.

Direction of discussion	Highlight	Ref
Integrity Framework	Merger of technologies to achieve data immutability and accuracy.	[92] [93] [94] [95] [96] [97] [98] [99] [100]
Regulatory Framework	Openness, transparency, anonymity, confidentiality, and security of user's information.	[101] [94] [95] [102] [96] [97] [103] [104] [105] [106] [107]
Scalable Framework	Transactional throughput, latency, information sharing, traceability, trust, and distributed storage.	[108] [93] [109] [110] [111] [101] [112] [95] [102] [96] [113] [114] [115] [116]
Privacy Framework	Privacy-preservation, access control, and interoperability.	[117] [23] [110] [118] [94] [96] [98] [119] [104] [120] [121] [122] [123] [124] [125] [82, 83]
Access Control Framework	Fine-grained access control, smart contract, decentralised secure identity authentication, verification, and monitoring.	[126] [127] [109] [112] [118] [94] [96] [73] [103] [105] [128] [129] [130] [131]
Service Availability Framework	Storage requirement, resource constraints management	[98] [132]
This work	Authorisation framework for ethical disclosure of private data in smart home healthcare using permissioned Blockchain as a service	

2.2. Related Work

Several studies in the field of smart home security, mostly focused 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 [8, 9]. 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 privacy framework proposed by the National Institute of Science and Technology (NIST) stated five core functionalities for achieving data privacy [133] 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 unauthorized access to user data [134]. Some even go as far as relating “Confidentiality” (which is a property of data) to “Privacy” (which is a property of an individual).

In handling privacy issues, all phases of the data value chain are to be considered, including acquisition/collection, analysis, storage, and usage. Two possible practical solutions are to implement privacy by design, and privacy-enhancing technologies [135]. Techniques often discussed to ensure privacy as illustrated in Fig. 10 include:

- i). Security, encryption, anonymization, and accountability controls (data provenance, policy enforcement, granular access control, accountability, and auditability).
- ii). Ownership, consent management, transparency, and control (privacy preferences, consent, sticky policies, personal data stores).

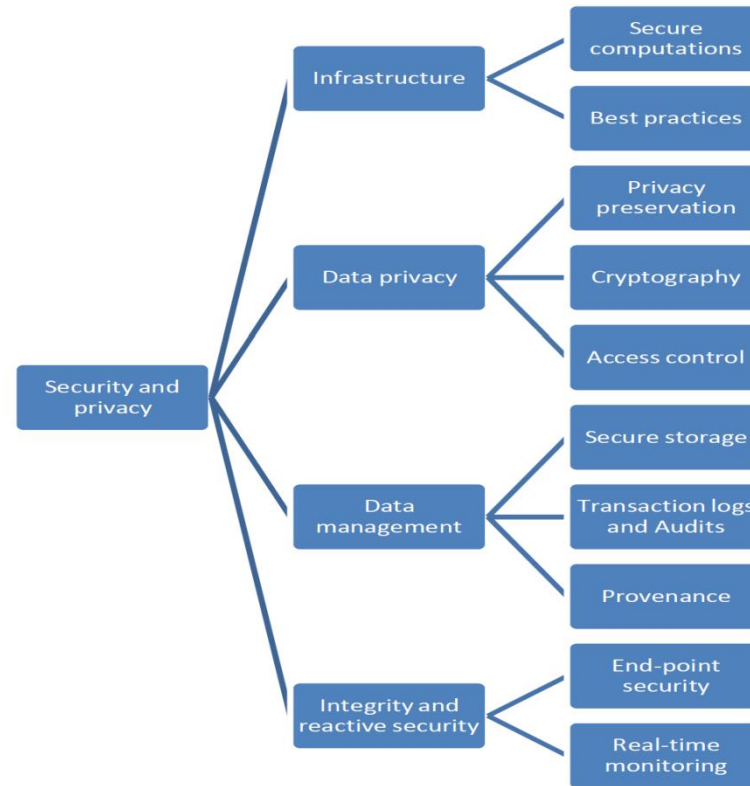


Fig. 10. Security and Privacy Taxonomy.

Furthermore, smart home system assets shown in Fig. 11 require intrusion detection and prevention against threats to the triad of CIA with emphasis on network and channel security as well. Mostly, recommendation techniques involve protecting the OSI seven layers to strengthen the security, tackle open internet connection issues, and reduce the risk of compromising a device on the smart home network [136], but traditional security measures are computational and storage intensive, energy-unfriendly for resource-constrained IoTs in smart homes.

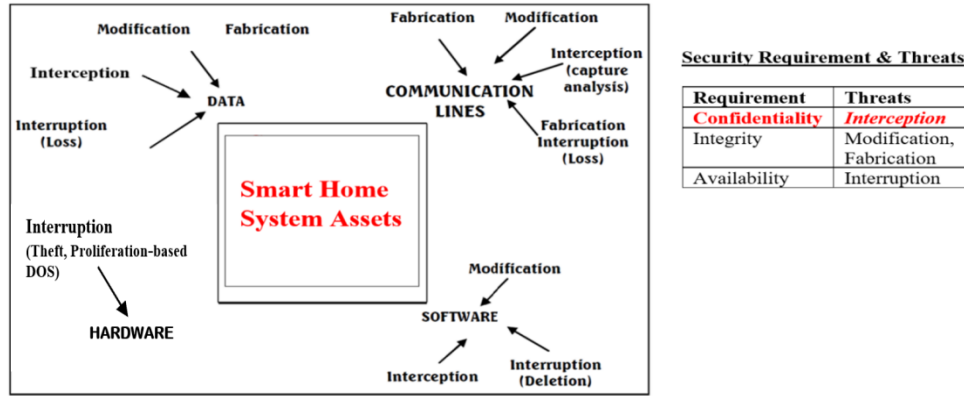


Fig. 11. Security Threats and Information System Assets in Smart Home.

Therefore, resource-friendly approaches for securing P2P network entities in the smart home ecosystem are beneficial to this study, and several related works are available in this regard. Specifically, the motive for using blockchain as a service is on the premise that the technology is built by providing asymmetric key encryption, hash values, and Merkle Tree in P2P networks as denoted in Fig. 12.

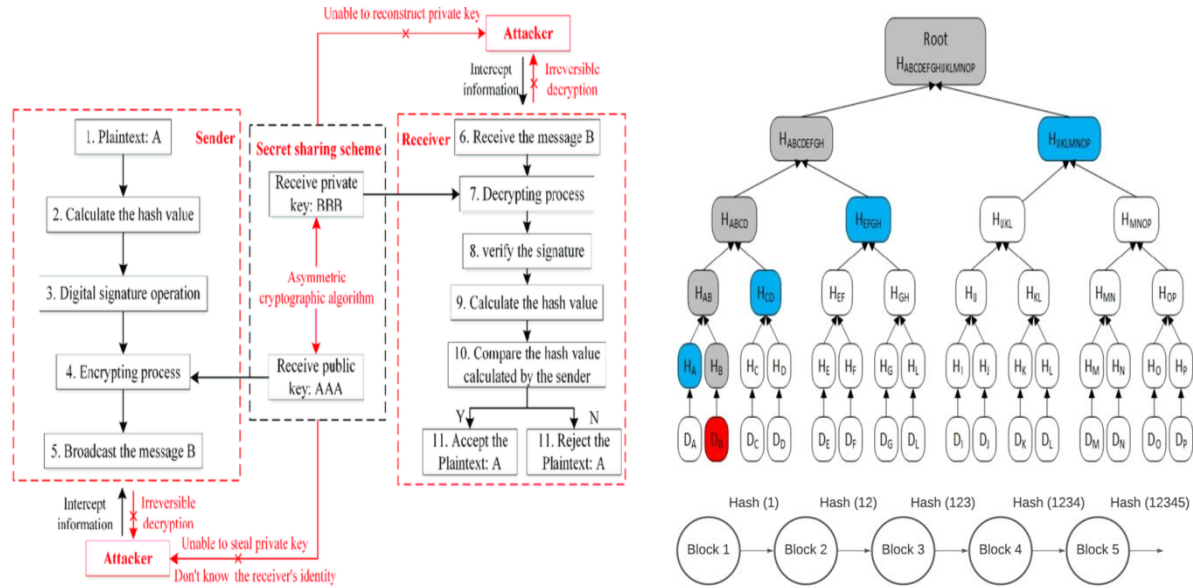


Fig. 12. Asymmetric Cryptography and Merkle Tree of blocks in the Blockchain [137].

In essence, the background study as illustrated in Fig. 13 examines lightweight methodologies and approaches that made use of cryptography primitives, access control techniques, artificial intelligence algorithms, blockchain technology, and references to other DLTs as these are state-of-the-art technologies utilised in tackling privacy deprivation concerns encountered in smart homes ecosystem. Furthermore, research agencies such as the Open Web Application Security Project (OWASP) [138] have identified privacy, insufficient authentication/authorization, lack of transport encryption, and poor physical layer security among the top ten vulnerabilities for IoT. Functional components of IoT reference architecture emphasized [139] identity management, authentication, authorization, key exchange and management, trust, and reputation, while major thrust area in the field of IoT security includes authentication, access control non-repudiation apart from confidentiality, integrity, and availability. Using cryptographic primitives all of these objectives can be performed. Confidentiality and integrity of the information can be achieved by cryptography. But traditional cryptographic methods require a large allocation of resources limited power supply, and limited battery life.

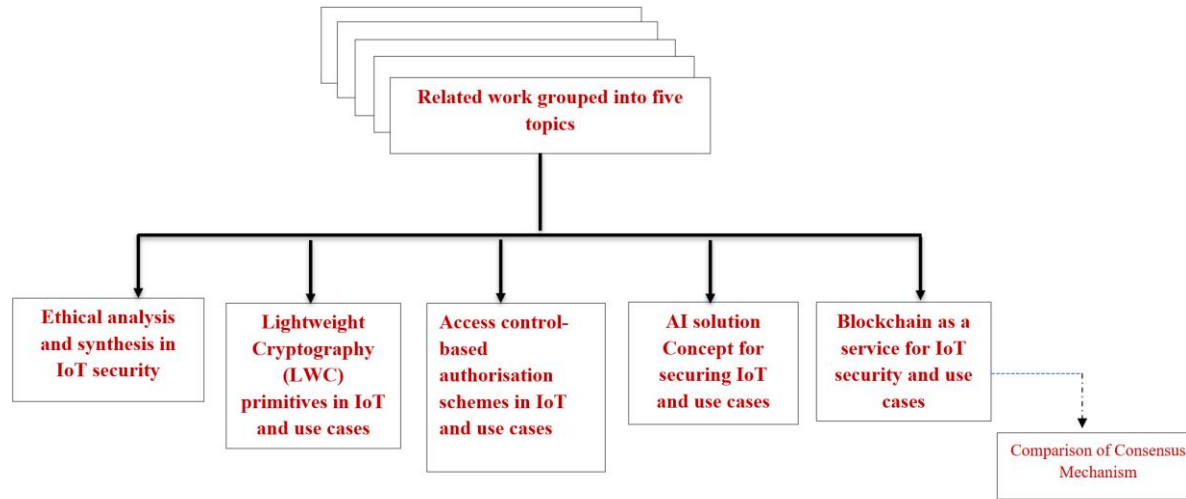


Fig. 13. Scope of related research work investigated.

2.2.1. Ethical analysis and synthesis in IoT security

There have been several attempts to address privacy issues anchored on ethics, mostly in the smart home context [140] where there are growing concerns about how collected data is used. This has been examined from a legislative viewpoint [141, 142], as well as from a technological standpoint. Authors in [143, 144, 145, 146] [144 -146] discussed privacy as what is ethically defensible in the context of the application. Specifically, [145] elaborated the architectural blueprint using legal concepts to propose the data subject's consent on personal identifiable information (PII) as a matter of control rather than trust and emphasized the principle of best practice for privacy by design (Art. 25 GDPR) using blockchain's hybrid cryptography to ensures individual data sovereignty and shared

transparency. The drawback is that the approach emphasized the non-legal argument which makes Blockchain data anonymous by reference, thereby making a consensus-centric, smart contract-enabled permissioned blockchain implementation a viable solution for securing private and sensitive data from the threat of data interception.

Government policy on public safety does not fully accommodate individual data ownership vis-à-vis data security and user privacy. Existing methodologies on privacy preservation struggle to protect citizens' data because some legislations support backdoor activities of government agencies (e.g., NSA) in the name of providing public security [144]. Cybersecurity Improvement Act emphasized IoTs should be patchable, devoid of known security vulnerabilities, and updatable, to forestall variants of Dyn's attack occurrence where ISPs experience a major Denial-of-Service (DoS) attack by an army of compromised IoT machines. Likewise, normative ethical considerations proposed in [119] focused on device manufacturers i.e., Original Equipment Manufacturers (OEMs), and stakeholders both on microscopic and macroscopic levels but had little or no consideration for end user's perception through end-user participation. Normative ethical consideration is proposed as a means of identifying the true human good (rightness and wrongness of actions) in software process enhancement and smart factories. Application of Teleological (consequentialist ethics) and Deontological ethic principles and theories are to serve as normative guidelines ab initio, with the recommendation of some defensible ethical obligations in smart factories deployment by stakeholders/protagonists. To make these comprehensively applicable in Consumer IoT, these exemplary and fundamental ethical considerations and recommendations will be adopted for privacy by design approach in this study. Authors in [147, 148, 149] emphasised the importance of ethics relating it to the transparency on the use of collected data based on the e-consent issue by the data owner as the reason for wanting to employ a DLT such as blockchain which has variants of consensus algorithm that make it applicable in the healthcare domain.

In [150] ethical considerations were discussed under two factors, i.e., those concerning privacy, social support, and autonomy; and the technology aspects of user context, usability, and training. The findings conclude that the older adult community is more likely to adopt assistive systems when the technology applied is personalised toward their needs, protects their dignity and independence, provides user control, and does not isolate them. Therefore, recommendations were made to researchers and developers of assistive technologies to assist those ageing-in-place in the adoption process [20]. Such recommendations bother on the following:

- Provision of interfaces via smart devices to control and configure the monitoring system with feedback for the user,
- Inclusion of various sensors/devices in designing a smart home solution to make it easier to integrate into daily life,
- Defining policies about data ownership.

2.2.2. Lightweight Cryptography (LWC) Primitives in IoT and Use Cases

Traditional cryptography techniques have played essential roles in ensuring data confidentiality and Integrity. Several research efforts have gone into adapting transport encryption schemes with resource constraints IoT devices (wearables) and BSN (nearables) used in digital healthcare delivery for the continuum of care. Moreover, asymmetric key encryption, hash values, and Merkle Tree or a binary hash tree are foundational and fundamental concepts to most distributed ledger technologies especially Blockchain in a P2P network. In [138] lightweight cryptography (LWC) primitives where Advanced Encryption Scheme (AES) and Elliptic Curve Cryptography (ECC) were highlighted as ultra-lightweight schemes suitable for resource-constrained systems. Consequently, BC implementations leverage hybrid cryptography in [151, 152, 153, 154, 155, 156] [151-156] to utilise lightweight symmetric techniques such as AES and Data Encryption Standard (DES); with emphasis on ECC as a more efficient LWC asymmetric approach and a suitable alternative to RSA because it requires a much smaller key size to provide the same degree of security for privacy by design, identity-based stateful encryption scheme, searchable encryption protocols, and unique data-dependent keys respectively. These methodologies achieved individual data sovereignty and shared transparency, computational efficiency that boosts secure communication, confidentiality, privacy-preserving encrypted queries, and the principle of least privilege. Authors in [157] revealed that primitive RSA is too hefty for IoT devices while ECC is lightweight but susceptible to replay and MITM attacks. Moreover, [158] argued that the use of LWC could assist in dealing

with traditional security, trust, and privacy issues in BCoT computing architecture for securing digital healthcare data and infrastructure. In [159], a privacy-aware PKI-based system developed for permissioned Blockchain proposed a digital certificate publishing scheme that assisted in preserving the privacy of user identity and provision of legitimate authorization. Discussion in [160] focused on the lack of security and resource efficiency as the two most important hindrances of large-scale application of any authentication scheme in the IoT network, making it difficult to find robust schemes appropriate for implementation in IoT networks. A three-factor ECC-based lightweight remote user authentication scheme for IoT networks was proposed to provide a legal mutual authentication between the remote user, sensor node, and gateway. An ECDH-based secure session key is established between the user and IoT node while authentication is done before the data collection via the gateway. The security analysis and formal verification performed using the AVISPA tool prove the resilience of the scheme against cryptographic attacks and demonstrate its lightweight compared to previous related schemes.

Arguments surrounding the integrity and confidentiality of medical information in the IoMT platform, an integration of IoT with medical systems used in medical applications for real-time diagnosis, remote patient monitoring, and real-time medicine prescriptions, etc., are of interest. The scenario is similar to that of a healthcare smart home in [161] which proposed a framework that encouraged ageing-in-place for the elderly via a caring network i.e., remote patient monitoring. The LWC-based data hiding (LWC-DH) system was proposed in [162] as a technique for attaining the security of patients' medical records to guarantee information confidentiality in IoMT by combining the LWC approach with a steganography model that ensures both secrecy and concealment to secure medical data. Elliptic curve cryptography (ECC) was used to encrypt even medical data while the odd ones with Feistel block cipher (FBC) cryptography. Lastly, the encrypted messages were hidden using redundant discrete wavelet transforms (RDWT) based steganography. The approach performed superior to contemporary schemes in terms of peak signal-to-noise ratio (PSNR), structural similarity index measure (SSIM), and mean square error (MSE) with better robustness, imperceptibility performance and low computation time as compared to traditional cryptography methods.

However, these aforementioned approaches did little to demonstrate an authorisation framework used for information disclosure and inherent control exercised by users which emphasised privacy by design, but only utilised a private key generator (PKG) which is an appealing single point of failure, presents issues of insecure key exchange among multiple entities in the presence of adversarial behaviours and had restricted application to non-sharable sensitive data respectively as limiting factors. Furthermore, suggested tactics in [163] proposed quality attributes for architecting IoT systems supported by Blockchain based on functional and non-functional security requirements. In line with this suggestion, hybrid cryptography was implemented using RSA-1024, AES-256, etc., for smart contract-enabled asymmetric or symmetric encryption, in combination with hash and digital signature algorithms such as SHA-256, ECDSA-SECP256K1 to ensure data confidentiality and integrity respectively in [121, 164] [165, 166, 167, 168, 169, 170, 171, 172, 173, 174] [165-174].

2.2.3. Access control-based Authorisation Schemes in IoT and Use Cases

Several approaches have been proposed to optimise access control schemes in smart home environments, which often involve many IoT devices with varying levels of trustworthiness. One approach that has been explored is the use of a private local Blockchain for access control of IoT devices in smart homes [165]. While this approach has the potential to provide distributed trust and privacy, it introduces latency due to the overlay tier and may be vulnerable to exploitation of transactions with public keys that are stored off-chain. Another approach involves repurposing Blockchain into a non-trust-based automated access control moderator that requires no trusted third party (TTP) and is associated with an off-chain key-value store, such as a Distributed Hash Table (DHT), for storing user's data, including location data [169]. However, this approach also has limitations, including the use of PoW consensus, which is computationally intensive and time-

consuming, and may not be suitable for resource-constrained smart home environments. In [175], a profile-based access control model (PrBAC) was proposed to minimise the issue of access control in a cloud environment. Before this implementation, Data Owners (DO) are required to be online always to supervise and oversee the permission granted to the user who wants to access data from a cloud server. With PrBAC, the data decryption key request-response process results in a secret key/password being issued to the user for the first and only time to gain access rights, making it unnecessary for the DO to be online always. Other benefits of the scheme reduced significantly the data access cost, and data access time, and minimised data redundancy. However, there is a huge scope of work to improve the confidentiality and security of the system. Moreover, the scope of the authorised framework for ethical disclosure of private data during patients' remote monitoring in the smart home healthcare ecosystem precludes the use of a cloud environment for the storage of sensitive well-being data. Instead, an IPFS that exhibits a similar ACID property and exhibits a relational off-shore versus on-chain relationship with Blockchain is more beneficial for the privacy-awareness concerns of this study.

In this context, the present review explores the Blockchain architecture that uses a lightweight consensus mechanism to securely manage data-sharing processes of resource constraints IoTs used in the smart home systems [170]. The examined PoA consensus algorithm is beneficial as it would handle transactions amongst the nodes in the smart home healthcare ecosystem at a higher rate, due to the absence of the mining process [168]. High scalability is achieved since blocks are generated in predictable sequence taking into consideration the number of validators, which are also pre-approved, thus allowing for greater efficiency and a higher throughput rate. The scenario presents a use case where the home node proposes a transaction, and some trustworthy nodes e.g., the storage or monitoring nodes, are randomly chosen (based on their reputation) to validate the transaction. The validator has the right to create blocks and add transactions to them as the Blockchain network builds up. Since the validation process is simplified, this algorithm only requires a limited number of block validators to maintain the network. Moreover, the use of inexpensive/high-ended nodes since mining is not required removes other complexities such as computational intensiveness observed in traditional consensus algorithms such as PoW and PoS. A beneficial trade-off possible with PoA is in sacrificing some characteristics of decentralization inherent in blockchain with gains of low overheads resulting in high transaction processing speed, high scalability, lower energy spends, and eco-friendliness as illustrated in Table 6.

The proposed solution assumes a scenario of adversarial behaviors within data generation, acquisition, collection, and transmission processes in a smart home healthcare ecosystem. It introduces lightweight transport cryptographic scheme systems for signing, authenticating, and verifying transactional data among network participants. Adequate algorithms would be designed for both off-chain and on-chain storage where incremental data and their hash values will be respectively. The framework offers several advantages, including the ability to achieve distributed trust and privacy, handle high transaction rates, and reduce energy consumption and computational requirements. Further research is needed to explore the feasibility and effectiveness of the proposed approach in real-world smart home environments.

Table 6

Comparison between PoW, PoS, and PoA Consensus Algorithms

Evaluation Parameter	POW	POS	PoA
Security	51% of the computing power is susceptible to attacking the network	51% of the network's wealth is susceptible to attack it	More centralisation, and risk of attack
Incentive	12.5 bitcoins and transaction fees of the product block (gas fee)	Transaction fees of the product block	Not applicable
Equipment	Computationally Intensive (requires computer power)	Does not require powerful and expensive hardware	Does not require powerful and expensive hardware
Energy consumption	High	Moderate	Low
Validation latency of transactions	High latency (about 10 minutes)	About six seconds to validate a block	Excellent, as it corresponds to network latency
Identity of the nodes	Public, fully decentralized	Random according to its wealth	Identity is a basic criterion for validator selection i.e., <i>identity-as-a-stake</i> .
Scalability	Excellent (thousands of nodes), Vertical	Excellent (thousands of nodes), Vertical	Unlimited and considerably scalable, Horizontal
Performance (throughput)	Low transactions and Performance, Limited due to the possibility of forking the BC	Comparatively lower transactions and Performance. Limited due to the possibility of the BC fork	High transactions and Performance. Excellent, due to tens of thousands of transactions per sec
Management of nodes	Accessible	Accessible	Authorised
Frameworks/platforms	Bitcoin	Ethereum, Peercoin	VeChain, Hyperledger fabric

Attribute-based access control utilised smart contracts for location sharing [176], and data privacy was achieved. The approach resulted in much lower computation overhead which met the set objective, except for query inefficiency (i.e., indirect query of Blockchain data), a challenge introduced by the misappropriation of on-chain/off-chain storage of transaction data. Permissioned Blockchain based on Practical Byzantine Fault Tolerance (PBFT) consensus algorithm and ECIES/AES in [167] provided traceability and privacy protection of access policy, both Blockchain and group signature were integrated to anonymously authenticate group members alongside the use of Message Authentication Code (MAC) to efficiently authenticate home gateway. However, fine-grained access control could not be achieved, and besides, PBFT employs PoW-like complex computations, where the efficiency degrades due to the high communication overhead that increases exponentially with every extra node in the network. Furthermore, Blockchain's smart contracts used ECDSA for verification and anonymity, but it rarely provided the identification assurance desired.

Another proposal implemented a publisher-subscriber algorithm [177] for notification to enhance a protocol for data access through smart contracts among providers and consumers of data in the eHealth realm because of the sensitivity of medical data. Only the response time (mining time), i.e., systems response time variation against the rate of transaction, was explicitly considered as a factor of performance evaluation of this approach among many other elaborate performance evaluation metrics such as packet and energy overhead that could ascertain the efficacy of such a proposal. Access control-based authorisation schemes in IoT [178, 179, 180, 181, 182, 183, 184] [178-184] proposed use cases in smart homes where authentication protocols/services were used to grant authorisation, access tokens, and tickets to build a system that ensures data security and user privacy. Blockchain was used for authentication i.e., user authentication scheme using Blockchain-enabled fog nodes where fog nodes interface to Ethereum smart contracts to authenticate users to access IoT devices. Such an authentication system

came with an overall system architecture, that is overloaded with the key role of different system participants i.e., Admins, End-users, SC, Fog nodes, IoT Devices, and Cloud.

Some other authorisation schemes used soft security mechanisms through rule and attribute-based access control such as belief and confidence score [183] for fine-grained access control to thwart insider attacks due to device sharing and the existence of complex social and trust relationships between entities. However, an external attack is more prominent due to the likely spread of the heterogeneous user entities that subscribe remotely to request personal transactional data of smart home subjects. Furthermore, the focus on trust rather than control is inadequate in the presence of adversarial behaviour, where only the data owner is judged to be the only entity that is not 'honest-but-curious', that is, the only trusted actor. Some other Auth schemes are mostly used and are efficient but utilise centralised authorisation schemes which makes them susceptible to a single point of failure (SPOF) attacks such as DOS.

2.2.4. AI solution Concept for securing IoT Edge devices

Artificial Intelligence (AI) solution concepts were proposed in [155, 185, 186, 187] for enhancing data security and privacy preservation in IoT-enabled ecosystems including smart home systems. In securing IoT edge devices, the AI Cyber Kill Chain model [185] was utilised with modules to detect, attribute, and identify stages of the attack life cycle. This solution is capable of handling/dealing with new threats or current versions of existing ones, including interception threats to data confidentiality. Despite the 84.7% success rate among peer techniques, the focus was on the edge layer and the evaluation metric was thematic. Various forms of interception threat could be detectable in the perception (sensing) layer of smart home devices as demonstrated but privacy concerns transverse the entire ecosystem of devices, communication, and services in smart homes. In Ambient Assisted Living [186], a solution that combined IoT technologies and machine learning to provide services that are context-aware and personalised, where anonymisation and data sharing were examined to develop a privacy-preserving model using machine learning and differential privacy. The privacy-preserving deep learning mechanism provided flexible anonymisation and data sharing, with evaluation methods that used various real and synthetic datasets. The technique, though exemplary in application, presented a passive control over user data privacy. Moreover, the application of differential privacy relates more to the public sharing of data and the non-interactive zero-knowledge proof concept.

Context-aware data allocation/controller mechanism via Fuzzy logic (AI) is utilised in [164] to effectively calculate the Rating of Allocation (RoA) value and extract each IoT data request based on multiple context parameters i.e., data, network, and quality used as threshold measurement, to assist with on-chain versus off-chain allocation decisions, focused in real-world healthcare application. Evaluation of the data allocation mechanism suggested improved network usage, latency, efficient Blockchain storage allocation to on-chain or cloud databases, and reduced energy consumption. However, the approach is best described as a reactive data allocation mechanism for calculating the RoA value, a dynamic and adaptive controller on how self-adaptive mechanisms and AI are needed to provide user privacy. An intelligent BCoT integration proposed in [28] presented a layered conceptual framework for smart applications to provide data reliability, privacy, and scalability by introducing an intermediary layer in the IoT ecosystem. The continuous stream of data generation, acquisition, manipulation, distribution, processing, and encryption among IoT devices is secured using a hybrid or private Blockchain network. The whole trusted data exchange and efficient storage involved the secure processing of all transactions with the introduction of a validator node in a P2P network.

Consequently, emerging studies in digital healthcare delivery have investigated the concept that combines blockchain, AI, and machine learning techniques [188, 189, 190, 191, 192] [188-192]. Smartly secured data privacy-preserving health monitoring in children [188] utilised blockchain to provide data security and avoided non-repudiation services while different ML algorithms were used to obtain the acceptable output with accuracy and performance measures; proposed a secure healthcare system using ML-based scalable Blockchain framework [189], examined Blockchain-AI implementation to securely store digital health records e.g. EHR (Electronic Health Records) and EMR (Electronic Medical Records) in eHealth systems [190, 193], maintain the source record to protect and preserve

the identity of patients, uncovered different ways of sharing a decentralized view of health information to improve medical accuracy, health, and prevent health disorders [194]. Evolving IoT-AI technologies in [191, 192] examined the potentialities of privacy-aware smart healthcare informatics. Blockchain-based federated learning (FL) in [195, 196] allowed for smarter simulations, lower latency, and lower power consumption while maintaining privacy at the same time to build a more reliable and robust IoMT model. Precision Healthcare (PHC) ineffectiveness due to challenges regarding low opt-in rates of patients was addressed with a Blockchain-enabled PHC ecosystem.

To fend against the resurgent threats posed by attackers, cyber-security professionals in [197] exploited AI methodologies that made use of the Ant Colony Optimization Convolutional Neural Network (ACO-CNN) mechanism. With the CNN algorithm, invaders and normal qualities were detected more successfully. More exact features were provided while subjecting chosen qualities to a training and testing approach, and performance metrics such as specificity, false alarm rate, recall, and accuracy were used for evaluation. With the developed framework, cyberattacks are detected more accurately by better-identifying intrusions and tracking attacker behaviour in the healthcare sector with more excellent performance. However, despite the numerous assault detection technologies and approaches, network infiltration is still unavoidable. Thus, a combination of advanced optimization with classification algorithms and future iterations of this approach is required to successfully detect more threats.

2.2.5. Blockchain as a service for IoT security and use cases

IoT, or the Internet of Things, represents one of the latest significant developments in the evolution of the internet. While it is not the final evolution, it is a major step in the ongoing transformation of the internet. IoT represents the next phase in this evolution. It involves connecting physical objects, devices, and sensors to the internet, allowing them to collect and exchange data. This connectivity enables real-time monitoring, automation, and the integration of the digital and physical worlds. IoT has found applications in various domains, including smart homes, healthcare, manufacturing, agriculture, and transportation. While IoT is a significant advancement, it is not the endpoint in the evolution of the internet. Technologies such as 5G, edge computing, artificial intelligence, and Blockchain are also contributing to the ongoing evolution of the Internet. These technologies are likely to further enhance the capabilities and reach of the internet, enabling new forms of connectivity, automation, and data processing. In essence, IoT is a significant step in the evolution of the Internet, but it is not the final evolution. The Internet continues to evolve with the integration of new technologies and innovations that expand its capabilities and potential.

IoT finds extensive applicability in numerous areas of healthcare. It helps patients get better treatment and medical facilities to function more competently. IoT in healthcare also enables machine-to-machine communication, information exchange, and interoperability which makes the delivery of healthcare effective. IoT can collect, report, and analyse the data in real-time thus removing the need to store the raw data. Applications in real-time monitoring via connected devices can save lives in emergencies like heart failure, diabetes, asthma attacks, etc. Other instances include, smart continuous glucose monitoring (CGM) and insulin pens (CGM) is a device that helps to continuously monitor blood sugar levels for several days, by taking many readings. Smartwatches are used to monitor depression, every year lots of people take treatment for depression. These watches detect depression levels and suggest what needs to be done for depression. This application assesses and monitors a patient's depression level and stores data in a cloud which enables psychologist to understand the patient's problem by monitoring from a distant place. Health data is one of the most valuable data and is highly sensitive. Therefore, patients' data are classified as personal or private data and are to be securely collected, stored, and accessed only by authorised personnel. Also, the issue of ethical disclosure comes in when the data owner's consent is sorted, programmed into the collection process, and managed through fine-grained access control by all information stakeholders to prevent indiscriminate use of patients' private data.

Blockchain is catalysing the transformational change in Industry 4.0, providing unparalleled security, authentication, asset traceability, access control through smart contract exchange, and ease of information exchange [198, 199]. Originally developed for cryptocurrency transactions, its usefulness has expanded through platforms such as Ethereum, which supports smart contracts and introduced a wide range of usability for private permissioned blockchain. These contracts consist of autonomous scripts that run on the blockchain, eliminating third-party intermediaries and reducing human-induced errors [200]. Such improvements ensure that communications are secure and transparent. Furthermore, the existence of multiple blockchain systems facilitates the integration of these smart contracts, moving Industry 4.0 into a new era of efficiency and trust [201, 202]. Blockchain integration in industry 4.0 is a game changer, revolutionising the centralised nature of various ecosystems by providing innovative infrastructure for developing robust distributed IoT-based applications including smart ecosystems in healthcare [203], finance, supply chain, cities, manufacturing, governance, agriculture, transportation, grid [204], education, e-Commerce, etc. The evolutionary adoption of blockchain applications in these sectors and their respective maturity trajectories from 2008 to 2023 are depicted in Fig. 14 and 15. Two of these sectors are duly discussed.

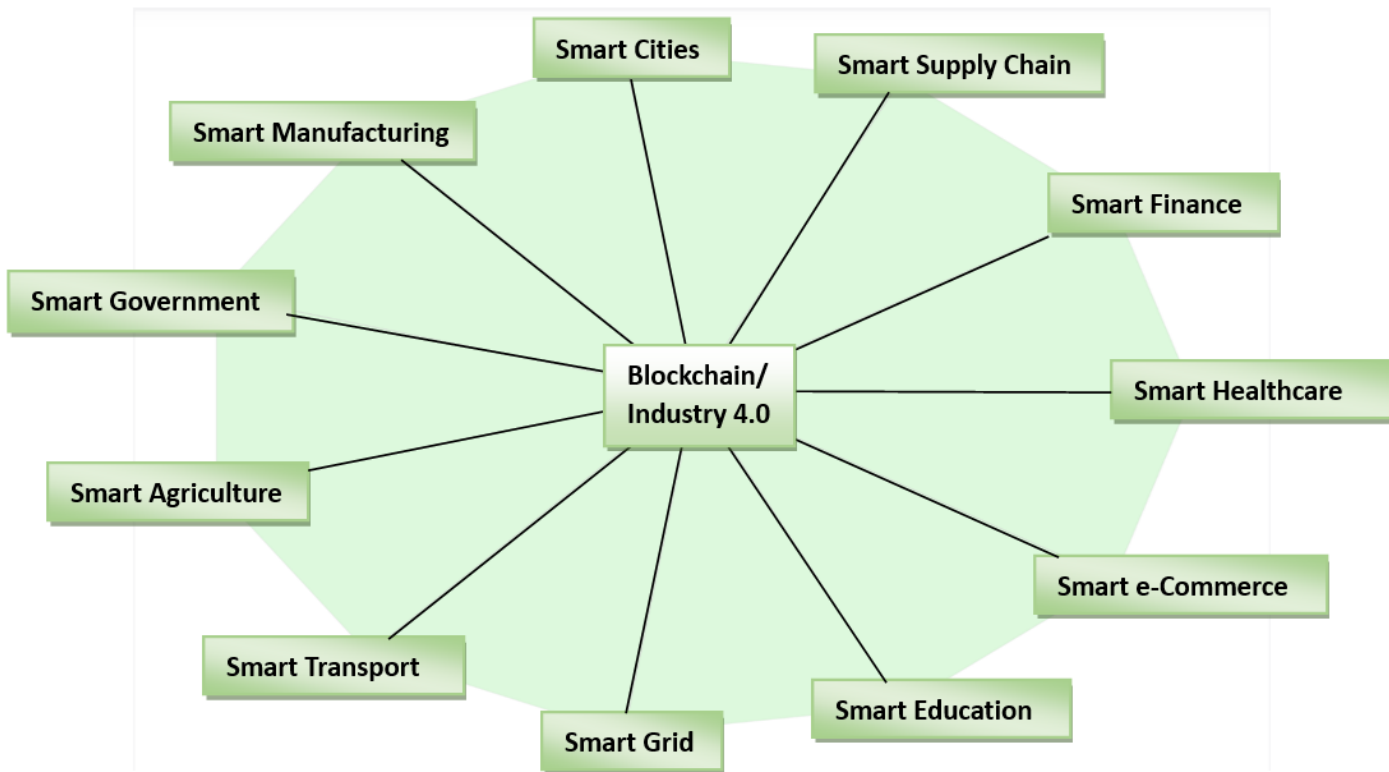


Fig. 14. Evolutionary adoption of Blockchain application in different sectors

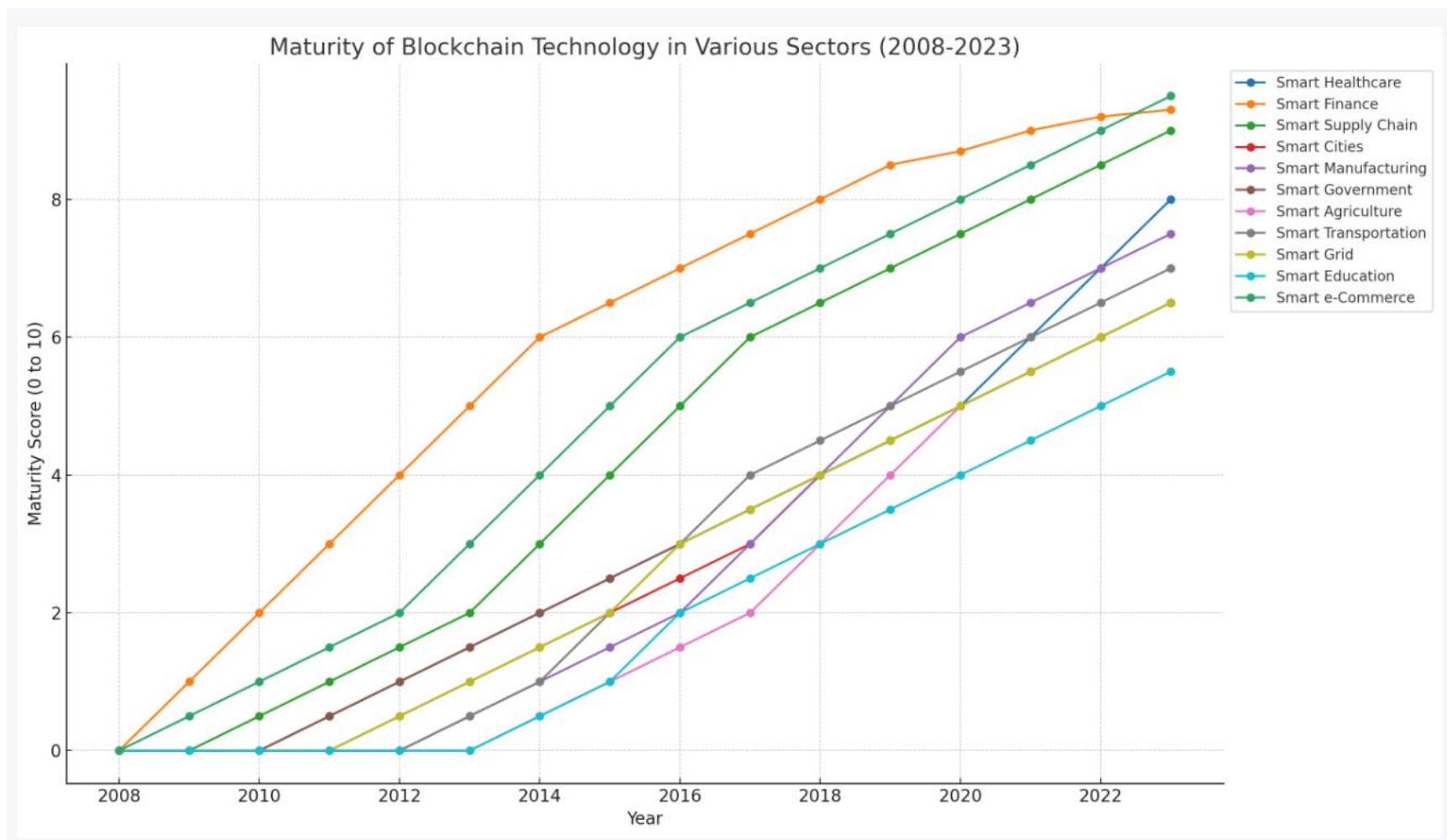


Fig. 15. Maturity of Blockchain technology across various sectors from 2008 to 2023.

VeChain in [205] is an instance of Blockchain usability in Industry 4.0. e.g., in the smart supply chain, manufacturing, and transportation. It introduces a value-seeking process for enterprise solutions i.e., a value chain that begins with provenance through ownership and authorisation to value exchange. Use cases of VeChain Toolchain integration are as follows:

1) Provenance for food & beverage supply chain e.g., Walmart China Blockchain Traceability Platform (2019).

2) Anti-counterfeiting and digitization for high-value products e.g., LVMH portfolio Luxury Maison (2016).

3) Digital vehicle passport: Stored and secured critical data on the VeChain blockchain across the entire lifecycle of the automobile. Examples include:

a) VerifyCar: BMW Group and VeChain's collaborative mission to counter odometer fraud in the secondary market. Use-case extendable to track the entire the health of individual cars by involving manufacturers, authorized repair shops, insurance companies, and financial institutions to upload, share, and verify data.

b) BYD, a leader in electric vehicle production, adopted the VeChain automobile lifecycle management solution which integrates mileage, electricity, and gas consumption data with the VeChainThor blockchain. Such information is used to compute the carbon emission reduction and reward the driver with carbon credits. To this effect, vehicle operators with carbon credits based on their vehicles' driving performance and carbon reduction are rewarded through the digital low-carbon emission ecosystem scheme. Hence, a solution with tools that introduces a blockchain-based ecosystem targeted at reducing the global carbon footprint. This is a use-case against climate destruction, where the footprint captured is recorded on the VeChainThor blockchain and made available to clients interested in participating in the initiative.

The white paper report in [206] demonstrated that the lightweights of Proof-of-Authority (PoA) consensus protocols in private permissioned blockchain are adaptable and suitable for the present study. It illustrated the value chain of provenance, ownership, and authorisation. Value exchange could mitigate issues of unauthorized identification (Sybil attack) as a threat to confidentiality in the smart home authorisation scheme. PoA-based Blockchain is not a censorship-resistant solution as observed in PoW-based Blockchain implementation where mining assists in validating transactions in a decentralized manner and is important for the integrity of a permissionless Blockchain where users are anonymous. Similarly, in Hyperledger, a permissioned Blockchain, nodes known to be trustworthy are assigned mining rights, and this is a beneficial concept to this study. PoA consensus mechanism is an ideal choice because of its high transaction rate to secure processes and use less energy. The privacy benefit of a permissioned distributed ledger is usable and applicable to the PoA consensus algorithm.

Blockchain is emerging as a beacon of hope in the realm of smart healthcare, addressing age-old challenges of secure medical record storage and privacy protection. With the need to always protect sensitive patient data, Blockchain provides an immutable, localized platform to ensure data integrity [207]. Moreover, its identity and management mean that only authorized personnel can access specific medical records, protecting patient privacy. Such improvements not only facilitate health care but also increase trust between patients and health care providers [208]. As the healthcare industry grapples with data breaches and privacy concerns, Blockchain's role in fostering a secure and patient-centric ecosystem is increasingly important. A use case is seen with ICON which was used to implement the largest Healthcare blockchain consortium in Korea, that is, Precision Medical Hospital Information System (P-HIS), which is joined by major domestic hospitals, with loopchain providing the underlying blockchain technology [209]. The goal of this is to build a permissioned network to share precision medical data securely, with a target to broaden the scope of medical data distribution globally through global networks, including OHDSI (Observational Health Data Sciences and Informatics). This consortium aims to build a safe and transparent distribution system of medical information based on blockchain, ensure interoperability between different hospital systems, manage access rights to data and records reliably, and promote the introduction of cryptocurrencies to the ecosystem. Other use cases of ICON include the capital market, insurance, university [210], and ICONLOOP, an expert in blockchain services in Korea in partnership with AWS [211]. Moreover, as shown in Fig. 16, the blockchain adoption journey is increasingly progressing to a reasonable level of maturity as new frontiers are been broken by researchers in this domain to tackle unresolved challenges including interoperability, survivability, manageability, and energy efficiency

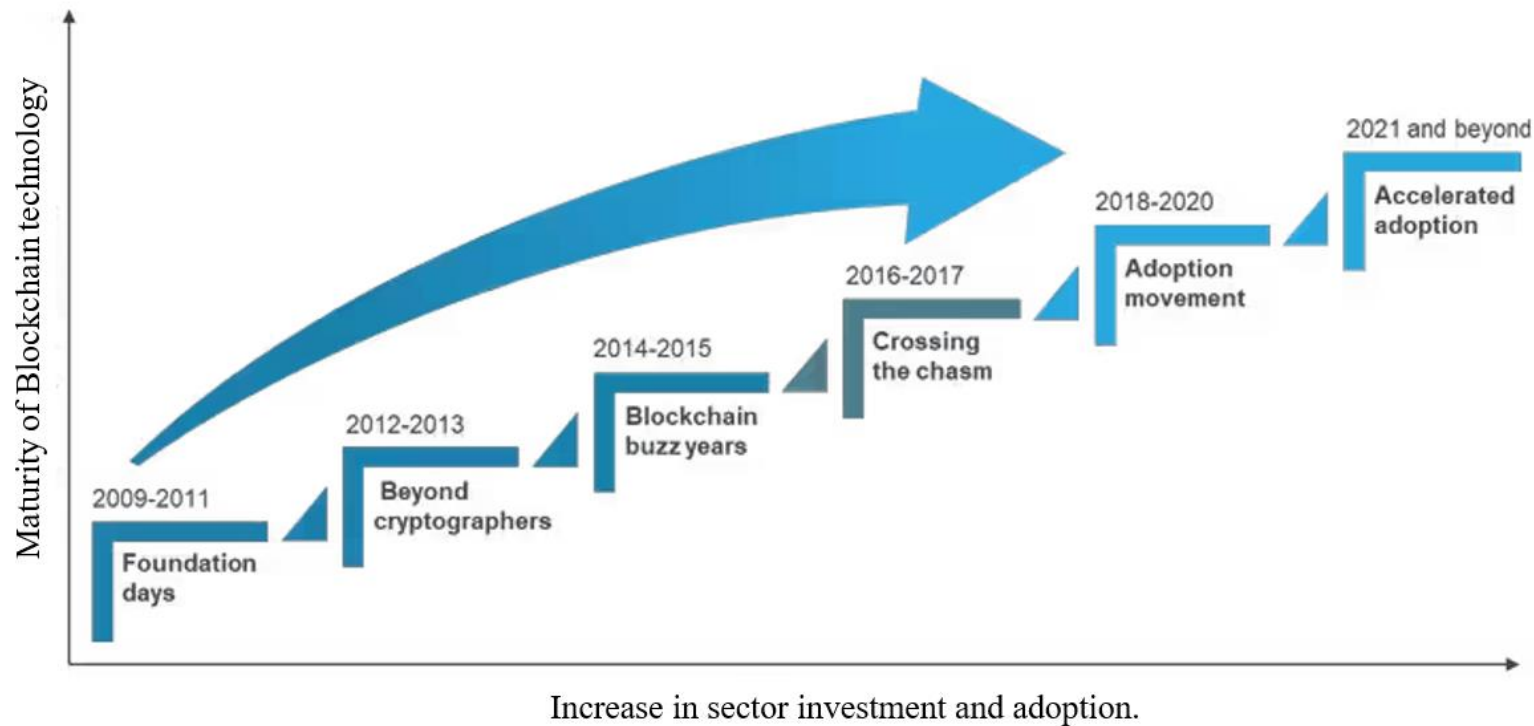


Fig. 16. Blockchain adoption journey [212]

Tactics suggested in [163] proposed quality attributes for architecting IoT systems supported by blockchain-based on functional and non-functional security requirements. It reiterated architectural decisions to consider in IoT systems supported by blockchain such as distribution of computation and storage (e.g., on-chain or off-chain), and BC Configuration (types of BC, data structure, and consensus protocol). It also identified gaps such as lack of focus on the following: architectural support for some quality attributes, integration of BC and IoT, etc., and threat types to validity e.g., external, internal, construct, and conclusion validity. Although no experimental testbed was used to shed light and evaluate the identified architectural tactics in terms of their most important trade-offs and dependencies, the principles enumerated will be of immense benefit to the current research in prototyping BC storage for transactional data and smart contract implementation.

In response to the challenges of security and privacy in IoT, researchers have explored the use of localized (private) blockchain technology as a viable solution. This approach offers several advantages, including the ability to safeguard data and transactions, as well as improve IoT security assessments, data integrity, and user privacy [213]. In particular, the PoA consensus algorithm is suitable for use in permissioned (hybrid) blockchain mechanisms as well. The application of such a tactically orchestrated consensus algorithm has been identified as an effective means of improving privacy preservation when Blockchain-based solutions with low overheads are required in smart home applications [163, 205, 206]. Unlike other consensus algorithms such as PoW, PoS, and PBFT, PoA algorithms are lightweight, censorship-resistant solutions with an inherent value chain of provenance, ownership, and authorization which further underscores its potential for securing smart home data transactions. Overall, the use of private blockchain technology and PoA consensus algorithms represent promising solutions to the security and privacy challenges associated with smart homes and IoT.

HomeChain in [167] utilized a permissioned BC based on PBFT consensus and Elliptic Curve Integrated Encryption Scheme (ECIES), an encryption standard based on the asymmetric key encryption algorithm, to ensure the confidentiality of the transmitted message. To further provide traceability and privacy protection of access policy, both Blockchain and group signature were integrated to anonymously authenticate group members alongside the use of a message authentication code (MAC) to efficiently authenticate the home gateway. The scheme chains all request records from group members, including revocation requests from the group manager to the BC, thereby applying Blockchain immutability and group signature traceability to make records tamper-proof as a measure of reliable behaviour auditing. Moreover, privacy protection of access policy is possible without the use of an access control policy table but through a revocation list to revoke the rights of malicious users. The technique implemented in HomeChain regarding privacy preservation is similar in scope but was performed using the Practical Byzantine Fault Tolerant (PBFT) Consensus Algorithm, which employs PoW-like complex computations, with a model that works efficiently only when the number of nodes in the distributed network is small due to the high communication overhead that increases exponentially with every extra node in the network; and is susceptible to Sybil attacks, and does not scale well because of its communication overhead (i.e., with all the other nodes at every step). The current study suggests a PoA consensus algorithm and ECC asymmetric encryption processes, which are more lightweight and handle data ownership of sensitive and private data more securely. Furthermore, the PoA consensus family i.e., based on Identity-as-a-stake, provides high performance and fault tolerance [30] more than PBFT.

Patient-centric access control in [214] utilised a combination of a private key, public key, and blockchain for remote patient monitoring, although with the downside of high computational and energy costs. Authors in [215] discussed the vital fusion of BC-IoMT as two emerging technologies integrated into a decentralised access control system with offers of privacy and security for the medical data of patients. Authors in [216] proposed a novel scalable framework shown in Fig. 17, that integrated IoT network with permissioned (Ethereum-based) blockchain in healthcare to address potential privacy and security threats for data integrity. Smart contracts handled device authentication, authorization, access control, and data management; off-chain data storage increased the overall scalability and privacy concerns of the model.

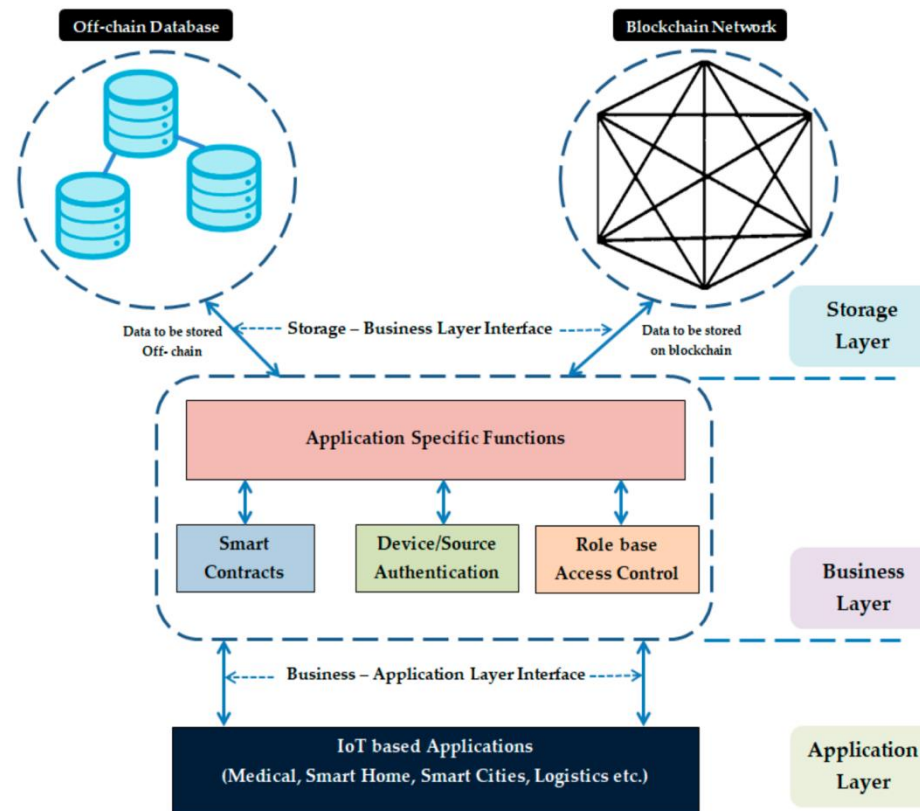


Fig. 17. Instance of Framework for BCoT Integration [216]

A risk analysis of the threats of Blockchain [217] investigated the role of blockchain in safeguarding health data, identifying related risks of blockchain technology implementation in the eHealth sector through an empirical study borne out of an extensive literature review, several authors' arguments, and examined discoveries. The study observed through semi-structures qualitative interviews the emerging concept of enhancing the Health Information Systems for storage and access control of health data for the continuum of care along the patient path, through the application of blockchain technology for Electronic Health Records, where existing centralisation of stored health data which represents a single point of failure and trust is adequately replaced with a secure decentralised approach built on consensus mechanisms and immutable chains of blocks for validating and securing data transactions. In line with seeking user opinion and perspective to enhance the concept of data security and privacy by design suggested in [146], eleven risks or threats to data integrity on blockchain systems identified by interviewees include amongst others poorly written smart contract code and misuse of the private key. The analysis revealed that only a permission Blockchain (private or consortium) seems appropriate for EMR/EHR implementation, Implementation recommendations suggest that storage and sharing of data can be handled

using off-chain storage such as IPFS, web3 storage, DHTs, etc., to add an extra layer of data integrity, while fine-grained access control is achievable through the implementation of multiple smart contracts to fulfill the EHR requirements. Thus, blockchain allows us to keep track of each patient's medical treatments, distribute data to relevant and authorized parties, and store the audit log. In addition, the study revealed that most threats arise from incorrect or incomplete data leading to insufficient data integrity. However, the disadvantage of high computational power requirements and scalability constraints are considerable threat factors in implementing traditional blockchain implementation in eHealth. Moreover, contrary to the limited view of the six interviews, a higher number of highly qualified participants would increase the number of identified threats and inaccuracy of some users' perceptions due to the language barrier.

The application of Blockchain in healthcare (BoHT) in [218, 219, 220, 221, 222, 223, 103, 224, 225, 226] [218 -226] revealed the dynamics of security and privacy frameworks possible with the integration of smart contracts, machine learning, signature algorithms, and consortium Blockchain architecture to protect the process for the collection, tracking, and storage of medical records pertaining to smart home healthcare systems. A summary of related works where the Blockchain-IoT framework has proposed privacy enhancement in healthcare record management using several emerging technologies is presented in Table 7. These innovations rely on the use of Blockchain and/or smart contracts as an integral building block for achieving various security objectives. The Internet of Things, on the other hand, has brought about dynamic growth in the digitisation of healthcare systems which enabled remote well-being monitoring and data collection procedures. Moreover, the IoT research space is increasingly attracting research interest that proposes the integration of various lightweight security techniques that could maintain the confidentiality and integrity of patients' personal and sensitive data from unauthorized tampering. Blockchain, digital signatures, smart contracts, multi-factor user authentication, etc., are emerging technologies being researched to secure IoT platforms and by extension smart homes equipped with sensors to render digital healthcare services. Table 8 is a comparison of related work and recent contributions to security objectives of privacy-preserving schemes within the IoT application domain.

Table 7
Comparison of related work

Blockchain-based													
Ref.	Architecture	Application Domain	Adversarial Model	SS	STT	EE	FT	TAI	CPA	AAAC	VIITU	TP	Limitations
[117]	Permissioned - Hyperledger Fabrics Smart Contracts	Electronic Health Record		√	√	√			P	AA	VI		No specific threat model addressed
[23]	ANCILE framework and Advanced Cryptography - Ethereum Smart Contracts	Electronic Health Record							P	AAC	VII		computationally intensive, arduous verification
[227]	Permissioned - Ethereum Smart Contracts	Electronic Health Record		√				√	CP	A		P	computational complexities.
[228]	Permissionless - MIT's publication on public BC	Medical Health Records		√				√	P	AC		√	The consensus algorithm used is not known
[229]	BC-IoT Federated Learning - Smart Contracts-based	Medical Health Records		√					CP	AA	VIU		Transacting nodes are not uniquely identified.
[134]	IoT, Cloud/Fog, Machine Learning, BC	Secure Embedded Living	External attack	√					CP	√	II		P4 lacks performance, and P4Runtime is vulnerable to MIT attacks and channel flooding.
[230]	Malware Recovery (MalRec) backup policies enforcement framework - Hyperledger Fabric, Smart Contract			√	√			√	CP	AA	II	√	Data verification is slow, the process could compromise the data's privacy

[231]	Private BC Benchmarking framework BLOCKBENCH - BC evaluation framework	Private BC Analytics		x	√	√						Considered three consensus algorithms for workload performance evaluation with little emphasis on privacy-related security requirements PoC, and Consensus Algorithm not specified
[177]	Private - Ethereum publisher-subscriber Smart Contracts	Smart Home Sensitive Data (eHealth realm) in Electronic Medical Records and Medical Big Bata.	Interception		√	√	CP	AAC	TU	P		
[232]	Consortium, Group signature, and asymmetric encryption. - PBFT & Hyperledger Fabric					√	CP					Deficient in handling the ownership of private and sensitive data
[167]	Group signature, and Message Authentication Code - Smart Contract, PBFT	Authentication System for Smart Homes	Impersonation, DDOS, Modification, Replay, MIIT Attack		√	√	√	A				PoC, Deficient in fine-grained access control
[233]	Permissionless, Merkel tree structure – Ethereum, smart contracts	Decentralized Smart Healthcare System (DSHS)		x	√	√	P		ITU	√		Unable to ensure efficient storage and integrity
[6]	Permissionless, Certificateless (ECC)	IoHT Realm	Myriad of Attacks e.g., Impersonation, Sybil, Replay attacks	x		√	PA		I			Inaccessibility of data due to inefficient data storage techniques.

Abbreviation	Property
SS	Secure Storage
STT	Scalability and Transaction Throughput
EE	Energy Efficiency
FT	Fault Tolerance
TAI	Traceability/Auditability/Irrevocability
CPA	Confidentiality/Privacy/Anonymity
AAAC	Authentication/Authorisation/Access Control
VIITU	Verifiability/Integrity/Immutability/Tamper-resistance/Unforgeability
TP	Transparency/Provability

√	Property satisfied
x	Property not satisfied
Alphabet	Indicating the security feature
	Property not specified or not applicable

Blockchain-based cont'd

Ref.	Architecture	Application Domain	Adversarial Model	SS	STT	EE	FT	TAI	CPA	AAAC	VIITU	TP	Limitations
[234]	Smart Home-based IoT-BC (SHIB) - Smart Contract, Ethereum	Smart Home Environment		√	S		√	I	P	AAC			Evaluation of latency awareness and energy spending not taken into consideration
[235]	Permissionless (ELIB) - Certificateless cryptography (CC), Distributed Throughput Management (DTM) scheme	IoT-enabled smart home environment		√	√	x			P	A	II		Inefficient energy consumption
[236]	Lightweight Scalable (LSB) - Distributed Time-based Consensus algorithm (DTC)	Smart Home Setting	Resilient to 8 relevant cyber attacks	√	√	√	√	√	√	A	√	P	Performance understanding based on PoC
[237]	Differential Privacy-based (DP-SGD), Attribute-based Access control, Edge computing, - Private Ethereum Smart contracts, ML Algorithm,	Smart Home Systems	Side channel, Modification, DoS, data mining, linking attacks	√	√			√	P	√	I	P	Loss of data and inaccuracy
[238]	Permissioned, PoA-based IoT, IPFS - Smart contracts Ethereum	Healthcare System - Disease Management	DDoS, Impersonation, Message forgery, MITT	√	√	√			√		VI		Lacks data filtering mechanism and real-time data analysis interface.
[239]	Consortium - privacy-preserving reputation systems	Analysis framework for privacy-preserving reputation systems	Adversary-dishonest participants					√	PA	A3C	√	√	The review acknowledged the exclusion of authorizability
[240]	BC privacy-preserving reputation framework (BPRF) - Group Signature Algorithm, Smart Contract		Abnormal behaviour (e.g., fake reports), Sybil attack	√	TT			√	PA			P	Smart contract not implemented
[241]	BC privacy-preserving Distributed Application (DA) to create and maintain healthcare certificates	Healthcare Document Management	Collusion, phishing, masquerade, Sybil						CP	A	V		It only considered medical certificate and mutual authentication via access control not achieved
[213]	Private (Local) - Decentralised Private BC	Smart Home Systems		√	√				CPA	AA			Limited Access Control Implementation

Abbreviation	Property
SS	Secure Storage
STT	Scalability and Transaction Throughput
EE	Energy Efficiency
FT	Fault Tolerance
TAI	Traceability/Auditability/Irevocability
CPA	Confidentiality/Privacy/Anonymity
AAAC	Authentication/Authorisation/Access Control
VIITU	Verifiability/Integrity/Immutability/Tamper-resistance/Unforgeability
TP	Transparency/Provability

√	Property satisfied
x	Property not satisfied
Alphabet	Indicating the security feature
	Property not specified or not applicable

Blockchain-based cont'd

Ref.	Architecture	Application Domain	Adversarial Model	SS	STT	EE	FT	TAI	CPA	AAAC	VIITU	TP	Limitations
[147, 148, 149]	Blockchain - Smart Contract Integration in Clinical Trial Data Security	Clinical trial complex data workflow encoding	Interception	√				T	P	AC	ITU	T P	Though aimed at privacy by design, implemented based on PoC using a fake experimental study
[166]	Blockchain-Based Multi-Level Location Secure Sharing Scheme.	secure location-sharing scheme							P	AC	VIIIU		Fnode (verifier) must not collude with LD, query inefficiency of light Location Demand (LD) nodes, PoW used to test the robustness of the scheme is computationally intensive.

Abbreviation	Property
SS	Secure Storage
STT	Scalability and Transaction Throughput
EE	Energy Efficiency
FT	Fault Tolerance
TAI	Traceability/Auditability/Irrevocability
CPA	Confidentiality/Privacy/Anonymity
AAAC	Authentication/Authorisation/Access Control
VIITU	Verifiability/Integrity/Immutability/Tamper-resistance/Unforgeability
TP	Transparency/Provability

√	Property satisfied
x	Property not satisfied
Alphabet	Indicating the security feature
	Property not specified or not applicable

Table 8

Signature-based Systems

Ref.	Architecture	Application Domain	Adversarial Model	SS	STT	EE	FT	TAI	CPA	AAAC	VI-TUI--IT	TP	Limitations
[242]	LSITA framework Neural Network – E-ECDH	Healthcare, IoT Communication	Interception	√					√	A	IT		logistic regression function used was sparsely done
[93]	Hash-based Message Authentication Code (HMAC) DS and BC's Smart Contracts	Healthcare IoT		√				√	C	A	√	P	The consensus algorithm & threat evaluation made unknown
[2]	Federated Learning (FL) and Ring-signature (FRESH)-Certificateless ring signature schema (ECC)	Smart Healthcare Systems							PA		V		Lacks incentive mechanism
[151]	Blockchain-enabled GDPR-compliant approach	sandbox for close collaboration between computer sciences and legal studies	Insider/external attack					T	√	AC	VT	√	blueprints for developers' solution compliance with the principle of Privacy by Design (Art. 25 GDPR).
[160]	ECC-based three-factor remote user authentication scheme	Smart device, IoT Service	Cryptographic attacks	S	TT				CPA	A	U	P	Exclusion of the gateway from data publishing is a security risk, limiting access control
[152]	identity-based and stateful encryption without complex certificate handling	Lightweight Encryption Scheme LES for Smart home system	chosen plaintext attack (i.e., IND-CPA secure)		TT				CP	A	I	P	Focused mainly on intruder attacks on resource-constrained devices
[243]	Advanced Lightweight Privacy-Preserving using PUF-based authentication protocol	Remote Health Monitoring	MITM, DOS, Replay, impersonation attacks					T	√	AA	I		Evaluation of noise consideration in PUF unknown as well as storage location of sensitive information
[183]	context-aware, behavior-based authorization framework	Home IoT Systems	Insider threat						CP	√	I		multiuser home IoT environment with user-centric anomalous request detection by the insiders not considered
[244, 41, 245]	Keyless Signatures Infrastructure Blockchain (KSIBC)	Hash-base e-health record management		√	√	√			CP	√	VIIIU		privacy of small data chunks through federated cloud missing

[246]	Enhanced Lightweight and Secure Certificateless Authentication Scheme (ELWSCAS)	IoT environment	KC, MITT, Replay, DOS, Eavesdropping, Impersonation	TT		I	CP	A	VI	P	Testbed limitation versus real-world IoT environment
-------	---	-----------------	---	----	--	---	----	---	----	---	--

Abbreviation	Property
SS	Secure Storage
STT	Scalability and Transaction Throughput
EE	Energy Efficiency
FT	Fault Tolerance
TAI	Traceability/Auditability/Irrevocability
CPA	Confidentiality/Privacy/Anonymity
AAAC	Authentication/Authorisation/Access Control
VIITU	Verifiability/Integrity/Immutability/Tamper-resistance/Unforgeability
TP	Transparency/Provability

√	Property satisfied
x	Property not satisfied
Alphabet	Indicating the security feature
	Property not specified or not applicable

2.2.5.1 Blockchain and the Battle Against Climate Destruction

In achieving net zero emissions by 2050, energy-efficient solutions are being offered by blockchain technology researchers. An open issue that has continuously hampered the adoption of blockchain technology is energy inefficiency. A concerted effort is ongoing to achieve an acceptable trade-off between performance and energy use, thereby making a blockchain that depends on mining to reach consensus (e.g., PoW) unsuitable for adoption considerations in any sector. Blockchain, after almost 15 years of growth and development has emerged as another disruptive technology that has further increased the energy spending experienced with the advent of the 4th industrial revolution (Industry 4.0), driven by corresponding advancements in the IT sector. In tandem with stages of industrial and digital transformation over the years, the Internet (web) has evolved significantly (from the 1980s to the 2020s) to what it is today, having gone through about five stages of technological integration (Fig 18). In considering the challenges of data integration, blockchain integration has contributed significantly to architecture and philosophies that shape the design of web products, providing various degrees of data security and management solutions to several emerging data-driven economies globally at a cost-energy spend. Consequently, data centre network energy spending is on the increase, accounting for 40% [1] excluding other hardware infrastructure, in an industry that has just about the highest energy consumption rate at par with the aviation sector, if it has not been surpassed [248, 249]. In a similar fashion to VeChain implementation in the automobile industry, authors in [250] deployed an architecture that utilised the Ethereum blockchain platform using a smart contract for business process improvement in the transportation sector thereby decreasing traffic congestion, reducing travel costs, and limiting energy consumption. The proposes a decentralized and secure cab-sharing system that provides ride-sharing services eliminating TTP, and by this means ensures the privacy of the driver's or rider's information, e.g., personal details, travel price, transit details, etc. The goal of the system is to secure user credentials through an algorithm that ensures verifiability, confidentiality, and unidirectionality features, and prevents collusion attacks; deploy a reputation score system with effective logistic matching performance to manage admin-user relationships; and reduce computational and communication overheads to ensure efficient system performance. Though the authors recommend the proposed encryption algorithm for implementation in domains such as IoT, big data, and healthcare, the design framework lacks an adequate authentication mechanism to complement the verifiability process in the proposed cab-sharing system. Moreover, the admin is a prominent attack surface, posing a SPOF threat. It is worth mentioning that though this study system is aimed at decreasing traffic congestion vis-à-vis reducing carbon emissions, lowering the carbon footprint in the blockchain industry is still a grave concern. Having recognised these concerns, there have been efforts within the industry to address the environmental impact. The ongoing transition to alternative consensus mechanisms, like Proof of Authority (PoA) or Delegated Proof of Stake (DPoS), which are less energy-intensive, is beginning to catch the attention of prospective users.

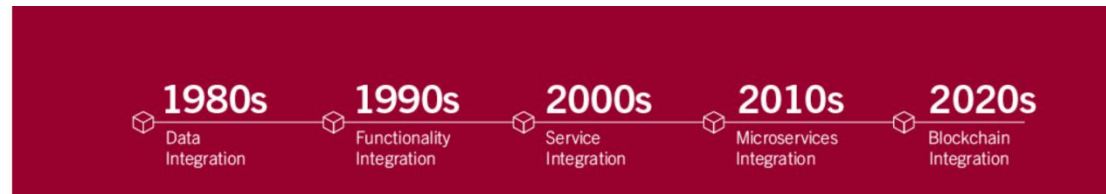


Fig. 18. Evolutionary trend from Data integration to Blockchain integration

The latest evolution of the Internet is the Internet of Things (IoT) and thereafter Internet of Everything (IoE). IoTs have been adopted in many sectors for data acquisition, data analytics, supervisory access control, automation, robotics (IIoT), etc. IoT and blockchain integration (BCoT) is a paradigm that has fostered Blockchain implementation in applications such as smart homes, smart healthcare, smart irrigation, smart traffic, autonomous vehicles, etc. All ranges of IoT devices (low, middle, or high-ended) are regarded as resource-constrained [251] in terms of energy, storage, and processing capability, and as such their integration requires a whole new thinking on energy management. However, these vast distributed connected devices could cumulatively consume a great deal of energy.

Having the right balance of performance versus energy consumption when implementing data security algorithms is essential. Resource-constrained IoT is susceptible to attacks due to the lightweightness of encryption schemes they can accommodate as opposed to the traditional cryptographic methods which employ high-ended and expensive hardware to achieve. This concept of robust hardware architecture made the traditional Blockchain performance savvy bit energy inefficient measuring cumulative energy spent in decentralised finance applications, a reputable source of studies and reports that specifically measure and analyze Bitcoin and Ethereum's energy consumption is the Cambridge Bitcoin Electricity Consumption Index [252]. Table 9 illustrates the historical Bitcoin and Ethereum network daily and annualized electricity consumption obtained from the Cambridge Blockchain network sustainability index.

Table 9

Instances of Blockchain Network Power Demand [252]

Cryptocurrency	Energy Rating/Time	Theoretical lower bound	Estimated	Theoretical upper bound
Bitcoin network power demand	Daily (GW)	8.73	14.18	25.09
	Annualised (TWh)	76.56	124.27	219.94
Ethereum network power demand	Daily(kW)	269.39	830.59	1984.62
	Annualised (GWh)	2.36	7.28	17.40

The transformative potential of blockchain technology promises more than just financial advancements; it holds the key to addressing some of the world's most pressing challenges, such as climate change [253]. However, the significant energy consumption of blockchains, especially those using the PoW consensus like Bitcoin, has been a cause for environmental concern [254]. Current estimations suggest that Bitcoin's energy consumption rivals that of some countries [255], leading to concerns about its sustainability amidst the global push for reduced carbon emissions. This has sparked ongoing research and debates among experts, advocates, and developers on transitioning from PoW-based blockchains to more energy-efficient consensus algorithms, such as Proof of Authority (PoA) [256, 257] or even considering alternative Distributed Ledger Technologies (DLTs) like Holochain [258, 259]. PoA-based authority master nodes in [260] can reduce energy consumption and enhance data security whereas a blockchain-based trust mechanism not only reduce energy issue but provide high-quality services such as security and data privacy in IIoT.

In the quest for net-zero emissions, the blockchain sector's current energy consumption cannot be ignored. Bitcoin's PoW consensus algorithm consumes 707 kWh per transaction [261, 30] and this is not sustainable and scalable. The broader adoption of DLTs in industries like healthcare, automotive, and supply chain [262] means that the cumulative energy usage can be substantial. Recognizing this, networks such as Ethereum are transforming to shift from energy-intensive PoW to Proof of Stake (PoS) [263], a more energy-friendly consensus mechanism. Such initiatives align with global carbon emission reduction targets and the broader goal of achieving net-zero emissions [264]. These shifts are not merely technical adjustments but resonate with the global urgency to combat climate change [265, 266]. However, the path to a greener blockchain is not limited to consensus algorithm modifications. Comprehensive approaches, integrating renewable energy sources [267], and promoting energy-efficient blockchain applications, are essential. For instance, while Bitcoin's energy consumption is often highlighted, many are unaware of the significantly lower energy requirements of networks using PoA, like certain configurations of Hyperledger Fabric [268]. By juxtaposing the energy consumption of PoW (Bitcoin-like), PoS (Ethereum-like), and PoA (Hyperledger Fabric-like) systems (Table 10), a clearer picture emerges, emphasizing the potential of transitioning to more sustainable DLT configurations [269].

Note as a clear disclaimer: The data used in Table 10 and graph in Fig. 19 are hypothetical and are meant for illustrative purposes. Actual energy consumption figures might differ based on numerous factors. However, the Cambridge Bitcoin Electricity Consumption Index [252] presents an actual energy consumption monitoring process that preludes that of PoA. Moreover, Fig. 20 is another realistic visualization produced by the UCL Centre for Blockchain on energy consumption comparison chart [270]. Proof of Authority (PoA) is inherently more energy-efficient than PoW, but quantifying the exact energy consumption for a PoA-based blockchain is challenging, and it would vary based on the specifics of the implementation, the hardware used by the validators, the network's overall activity, and other factors. There is no widely recognized and dedicated site similar to the CBECI that tracks energy consumption specifically for PoA-based blockchain systems. Most of the discussions around blockchain energy consumption focus on PoW because of its significant energy demands. PoA, being more energy-efficient, does not attract the same level of scrutiny or detailed tracking. Some individual projects or chains that utilise PoA might provide their energy consumption estimates or benchmarks, but these would be specific to that particular chain and not a general measure of PoA's energy consumption.

Table 10

Comparison of energy consumption of different consensus mechanisms

Consensus Mechanism	Estimated Energy Consumption (TWh/year)
Proof of Work (Bitcoin-like)	120
Proof of Stake (Ethereum 2.0-like)	5
Proof of Authority (Hyperledger Fabric-like)	0.05

Fig. 18 illustrates the energy consumption trends of different consensus mechanisms from 2010 to 2022:

- PoW (Bitcoin-like): As shown in red, the energy consumption for PoW mechanisms has seen significant growth, plateauing in recent years. This reflects the massive energy requirements of networks like Bitcoin, which rely on PoW.
- PoS (Ethereum 2.0-like): The blue line shows the energy consumption for PoS mechanisms, which, while growing, remains significantly lower than PoW. Ethereum's ongoing transition to PoS is a notable example of this shift towards more energy-efficient consensus mechanisms.
- PoA (Hyperledger Fabric-like): The green line represents PoA, which consumes minimal energy compared to PoW and PoS. It has been stable over the years, indicating a consistent, low energy footprint.

This visualization underscores the need for the blockchain industry to steer towards more sustainable consensus mechanisms, especially as DLTs find more extensive applications across various sectors. By adopting energy-efficient solutions, the blockchain ecosystem can contribute significantly to global efforts against climate destruction.

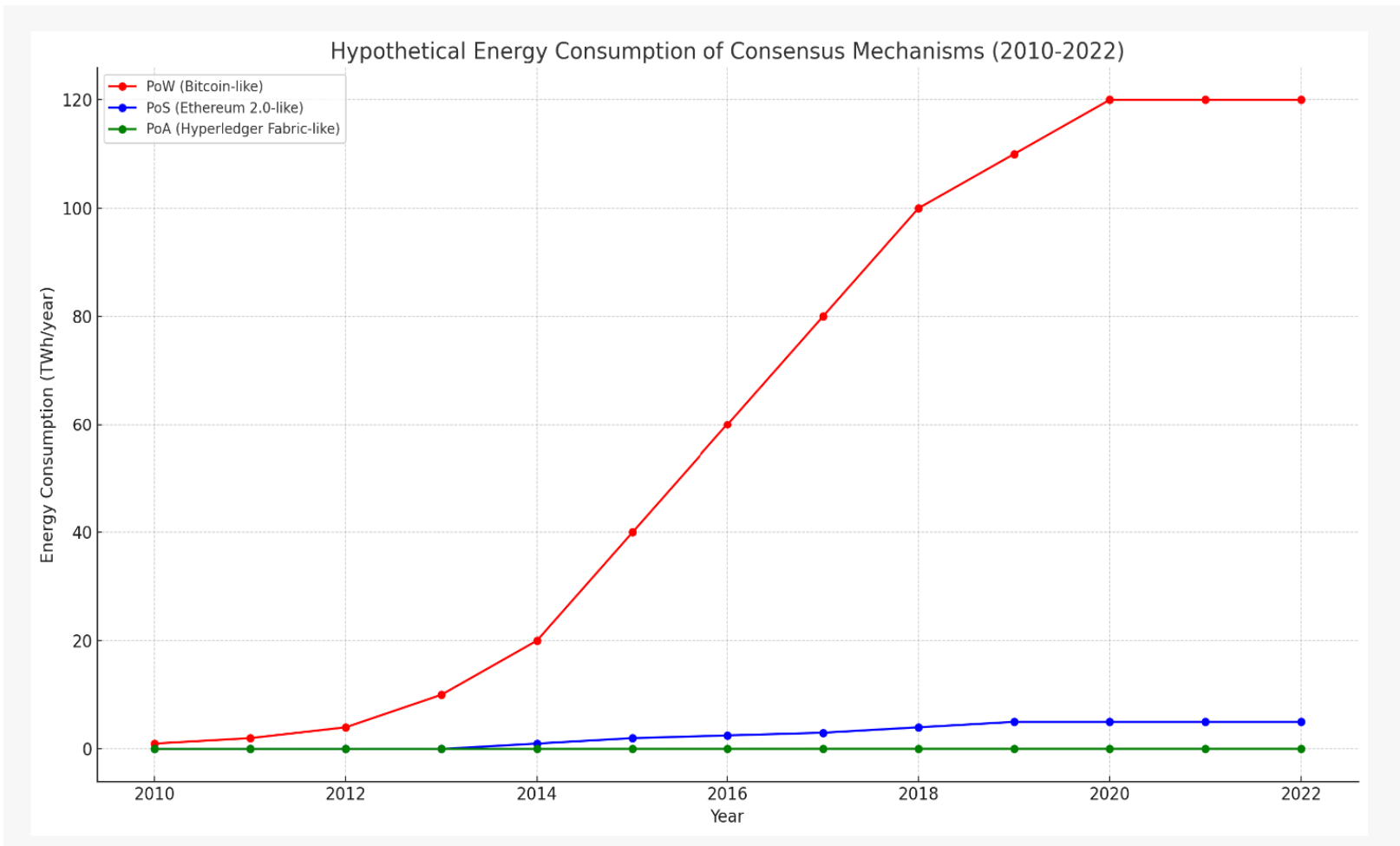


Fig. 19. Illustration of energy consumption trends of different Blockchain consensus mechanisms from 2010 to 2022

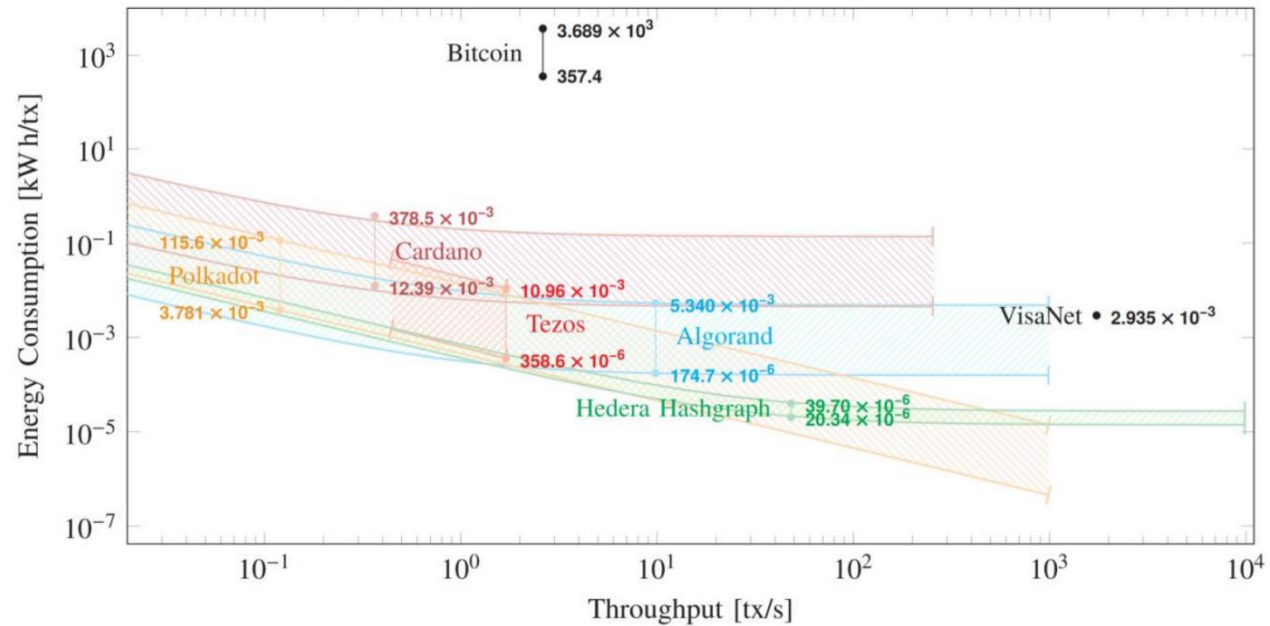


Fig. 20. Energy consumption comparison chart [270]
 Courtesy: UCL Centre for Blockchain Technologies)

Metrics used to measure the energy efficiency of blockchain algorithms compare the Energy Consumption per Transaction (ECT) – the amount of energy required to process one transaction on the blockchain, and the Energy Consumption per Second (ECS) - the amount of energy consumed by the network in one second, to evaluate how much energy is wasted or conserved by different algorithms. For instance, estimates of the ECT and ECS of Bitcoin's algorithm (PoW-based) and that of Ethereum's algorithm (PoS-based) can be computed from the Bitcoin Energy Consumption Index (BECI) and the Ethereum Energy Consumption Index (EECI) respectively. Alternatively, online calculators or simple formulas usable to compute the ECT and ECS of different algorithms include:

- For ECT of Bitcoin's algorithm: $ECT = ECS / TPS$

Where ECS is in kilowatt-hours (kWh), and TPS - the transactions per second processed by the network.

- To calculate the ECS of Bitcoin's algorithm: $ECS = H * P / E$

Where H is the hash rate in tera hashes per second (TH/s), P is the power consumption per hash in joules (J), and E is the energy efficiency in joules per kilowatt-hour (J/kWh).

2.2.5.2 Comparison of Blockchain with other DLT applications - Holochain

Recent advancements in distributed ledger technologies (DLTs) have prompted researchers to explore novel approaches to ensure data privacy and security in the healthcare sector. While blockchain remains the most widely recognized DLT, characterized by its immutability and decentralized consensus mechanisms, its limitations have become apparent, especially in contexts demanding high scalability and more granular data sovereignty [269]. These concerns have led to the rise of Holochain, an emerging technology that adopts an agent-centric approach, whereby each participant maintains their chain, thus allowing for more scalable and adaptable solutions [271]. Holochain's design does not necessitate global consensus, potentially offering enhanced efficiency and reduced energy consumption compared to traditional blockchain systems [272].

Furthermore, the healthcare sector, characterized by its need for secure, real-time data sharing and stringent privacy standards, stands to benefit from the unique features of Holochain. Sensitive patient data, requiring stringent access controls, may be better managed through Holochain's agent-centric model, ensuring that only authorized entities can access specific datasets [273]. Additionally, Holochain's modularity can support varied healthcare applications, from patient record management to real-time monitoring [202]. While blockchain's merits, particularly in terms of data integrity and transparency, remain undeniable, researchers and practitioners need to consider the potential of Holochain as an alternative or complementary solution in the quest for optimizing healthcare data privacy and security [275, 276]. Advantages of Holochain over Permissioned Blockchain with Proof of Authority (PoA) for Smart Home Healthcare Ecosystem:

- i). **Scalability:** Holochain is designed to be more scalable than traditional blockchains. Since it does not require global consensus, there is no need for every node to process every transaction. This can be advantageous in a smart home scenario where numerous devices may be making frequent data updates.
- ii). **Energy Efficiency:** Holochain does not employ energy-intensive consensus mechanisms like Proof of Work (PoW). Although it is compared to PoA, which is also more energy-efficient than PoW. Holochain's lack of a need for consensus at all can be seen as a plus in terms of energy usage.
- iii). **Data Sovereignty:** Holochain emphasizes agent-centricity, meaning each participant (or device) in the network has its chain. This can ensure that devices in a smart home can have their data histories, ensuring more granular control over data.
- iv). **Modularity:** Holochain allows for the creation of different 'hApps' or Holochain applications, which can be useful for different functionalities within a smart home system.
- v). **No Cryptocurrency Requirement:** Unlike many blockchain systems, Holochain doesn't inherently require a cryptocurrency to function. This can be useful in scenarios where token economics might be complicated or not necessary for the intended application.

In considering Holochain for secure data management in smart healthcare systems, it is well known that Holochain is gaining attention as an alternative to blockchain for various applications, including those related to privacy and security. Here is why it might be worth considering for a healthcare system:

- i). **Fine-Grained Access Control:** Holochain's architecture allows for detailed and specific rules about who can access what data and when. This can be crucial in healthcare, where specific patient data might need to be shared with certain professionals but not others.
- ii). **Data Redundancy:** Holochain's DHT (Distributed Hash Table) ensures that data is redundantly stored across nodes, which can add resilience to the system. This might be crucial for critical healthcare data.
- iii). **Interoperability:** Holochain's modular approach can be advantageous for integrating various healthcare systems or platforms.
- iv). **Data Authenticity:** Since every agent has its chain, it is easier to verify the source and authenticity of data, which is crucial in healthcare scenarios.

- v). **Less Centralization:** While PoA blockchains can offer efficiency and scalability, they might also introduce central points of control or failure. Holochain's design minimizes centralized control.

However, it is worth mentioning that every technology has its trade-offs. Therefore, for specific use cases, a permissioned Blockchain with PoA might offer benefits in terms of established infrastructure, easier integration with existing systems, or specific security guarantees. When considering any technology for such a critical application, it is vital to conduct thorough research, testing, and validation to ensure it meets the required needs and standards. In developing an authorisation framework, fine-grained access control [169, 177] was achieved using a publisher-subscriber smart contract to ensure privacy, trust, and decision-making in Blockchains. Therefore, implementing a PoA-based and smart contract as a 2-in-1 approach to ensure consent-based disclosure of private information could be more beneficial than relying solely on Holochain for all the privacy-preservation requirements in the smart home healthcare ecosystem. Using a publisher-subscriber smart contract model atop a blockchain that implements the PoA consensus algorithm can indeed offer fine-grained access control, and in many cases, this might be an excellent solution. The advantages (Fig. 21) and potential challenges of such an approach include:

Advantages:

- i). **Consent-Based Disclosure:** Smart contracts can be coded to ensure that access to specific data requires explicit consent from the owner (publisher) of the data. This provides a clear mechanism for consent-based disclosure.
- ii). **Transparency and Immutability:** The use of blockchain ensures that all interactions (such as granting or revoking access) are recorded on an immutable ledger. This can be particularly important for auditability and traceability in healthcare scenarios.
- iii). **Established Infrastructure:** Many enterprise blockchain solutions that use PoA already have infrastructure, tooling, and libraries in place to facilitate the creation and management of smart contracts.
- iv). **Security Guarantees:** PoA blockchains can offer specific security guarantees due to their consensus mechanism, and if managed correctly, they can mitigate the risk of malicious actors.
- v). **Integration with Tokens:** If needed, tokenized incentives or payments can be seamlessly integrated into the publisher-subscriber model on a blockchain.

Potential Challenges:

- i). **Scalability Concerns:** While PoA blockchains can handle a higher transaction throughput than, say, PoW systems, they might still face scalability issues, especially if the smart home healthcare ecosystem has numerous devices producing a large volume of data transactions.
- ii). **Centralization Risks:** PoA systems introduce validators or authorities that have the power to validate or deny transactions. This can introduce central points of control or failure.
- ii). **Complexity:** Implementing a publisher-subscriber model with all the necessary privacy and consent features on a blockchain might be complex and require rigorous testing to ensure no vulnerabilities.
- iv). **Potential Latency:** Depending on the implementation and the number of authorities in the PoA system, there might be a latency in recording and validating transactions, which could be a concern in time-sensitive healthcare scenarios.

Holochain in Comparison:

Holochain's agent-centric approach inherently provides each agent (or device) with its chain, making consent-based sharing more intrinsic to its design. However, it is a newer technology compared to many blockchain solutions, and its adoption in critical applications like healthcare would require thorough vetting. Therefore, the suggestion of using a 2-in-1 approach with a publisher-subscriber model on a PoA blockchain is certainly valid and might offer the right balance of transparency, control, and security for a smart home healthcare ecosystem. However, the best choice often depends on the specific requirements of the system, including factors like transaction volume, required response times, and the existing technological infrastructure. Both blockchain and Holochain have their merits, and a hybrid approach, or even using them in tandem, might also be worth exploring.

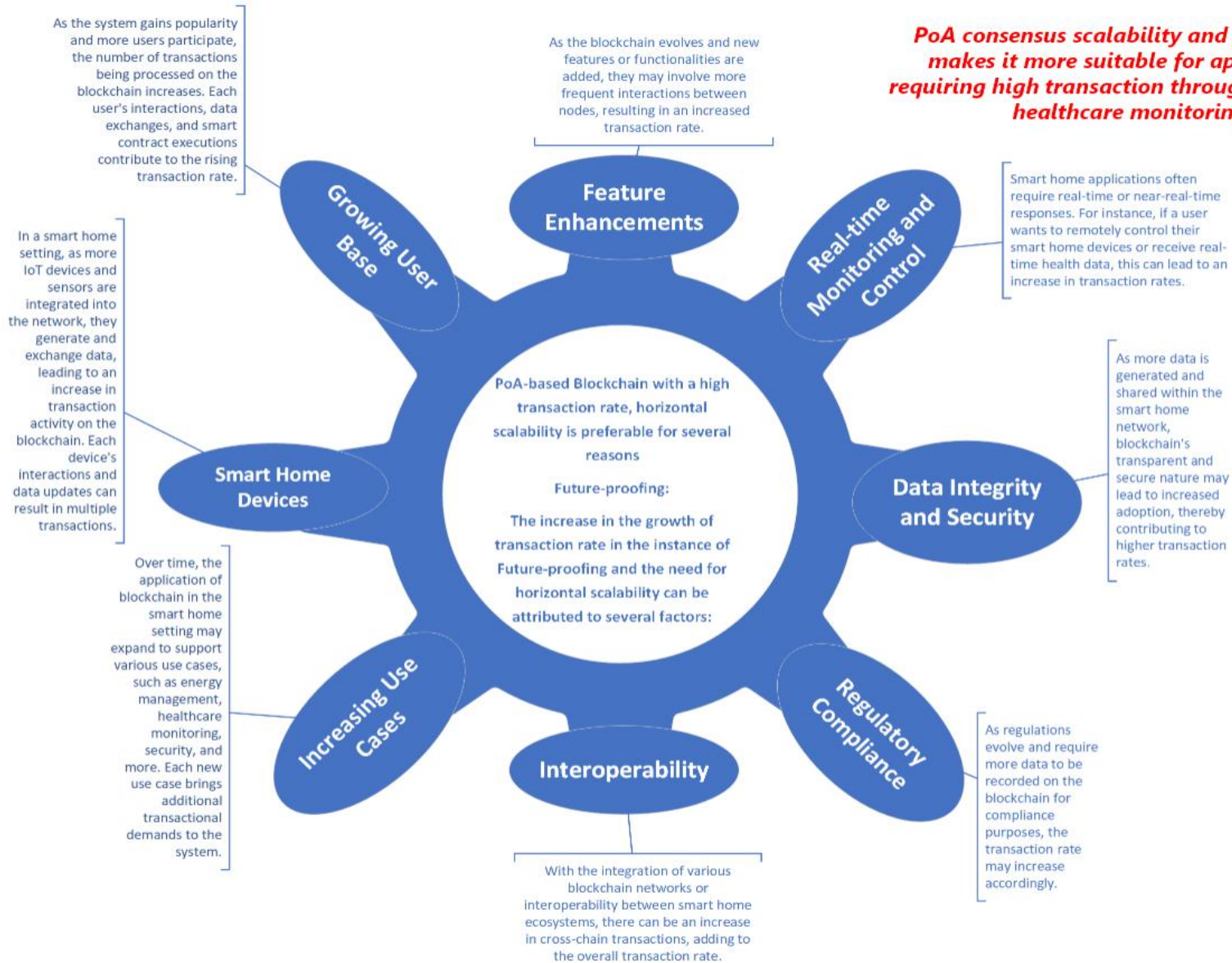


Fig. 21. PoA characteristic of scalability and high transaction throughput

2.2.5.3 Hybrid approach – Blockchain and Holochain

Combining the strengths of both blockchain and Holochain can yield a robust system, especially in a domain as critical as healthcare, that is, in the smart home healthcare ecosystem as regards privacy preservation of healthcare users and their data security. Here are some methodologies to consider:

1. Layered Architecture:

- **Blockchain Layer:** This layer can be used for storing critical, immutable records like patient consent forms, treatment history, or medication logs. The blockchain's strength in transparency and immutability can be leveraged here.
- **Holochain Layer:** This layer can manage more dynamic and frequent data updates, like real-time health metrics from wearables or smart devices. Holochain's scalability and agent-centric approach can ensure real-time data processing without overburdening the system.

2. Dual Validation:

For highly sensitive operations, both systems can be used to cross-validate transactions.

- A transaction (like granting access to medical records) is first validated in the Holochain network.
- Once validated, it is recorded in the blockchain for added immutability and traceability.

3. Decentralized Identity Management:

- **Blockchain:** Use blockchain to manage decentralized identities of patients, healthcare providers, and devices. This ensures a tamper-proof identity system with clear audit trails.
- **Holochain:** Use Holochain to manage permissions, access controls, and dynamic data sharing based on these identities.

4. Data Segregation:

- **Blockchain:** Store summarized or aggregated data, which can be useful for research, public health insights, or statistical analyses without revealing individual data.
- **Holochain:** Store detailed, individual-level data, ensuring only authorized entities can access specific granular data.

5. Smart Contract Coordination:

- **Blockchain:** Implement smart contracts to automate consent-based data sharing, payments, or other predefined actions in the healthcare ecosystem.
- **Holochain:** Validate and execute the outcomes of these smart contracts in real-time, using its efficient processing capabilities.

6. Backup and Redundancy:

- **Blockchain:** Use as a backup system to periodically store snapshots of critical data from the Holochain network. This ensures data longevity and a recovery mechanism.
- **Holochain:** Handle the real-time, dynamic operations and data flows of the healthcare ecosystem.

7. Token Integration:

- **Blockchain:** If there is a need for token-based incentives, payments, or penalties, this can be managed on the blockchain layer.
- **Holochain:** While Holochain does not inherently require a token system, it can recognize and respond to token-based actions initiated on the blockchain.

8. Interoperability Bridges:

- Develop bridges or middleware that allow smooth data and transaction flow between the blockchain and Holochain networks. This ensures the two systems can effectively communicate and collaborate.

9. Data Encryption and Security:

- Blockchain: Implement strong encryption for data stored on-chain, ensuring only authorized entities can decrypt and access it.
- Holochain: Use its agent-centric model to ensure data sovereignty and fine-grained access controls, complemented by encryption for added security.

10. Audit and Compliance:

- Blockchain: Regularly record audit logs and compliance checks to the blockchain, ensuring a tamper-proof history of all system activities.
- Holochain: Used to manage and execute real-time compliance checks, automating many aspects of healthcare regulatory adherence.

In essence, the methodologies revolve around leveraging the strengths of each system where they shine best and ensuring they complement each other. Such a hybrid approach requires careful design, thorough testing, and continuous monitoring to ensure the privacy and security of healthcare users and their data. Moreover, a private Blockchain scheme (PoA-based) is highly favored for the combination of these two technologies to drastically reduce likely complexity that could result, including energy efficiency.

2.2.5.4 Blockchain Risks and Mitigating Techniques

There are various risks associated with introducing blockchain technology to most organizations. The following are the most encountered risks: strategic risk, information security risk, operational and IT risk, business continuity, supplier risk, key management risk, data confidentiality, and security risk. Thus, organizations should be prepared to encounter these risks and should implement a higher level of risk management. The three main domains of risk are as follows:

Standard risks:

The stage at which the institution aims to adopt blockchain technology, the choice of the network in which the participants must be, and the constraints in the products being developed in the existing platform are covered under strategic risk. As blockchain technology reduces the period of processes involved in the business, the business continuity plan should ensure minimal response and recovery time even if it fails. Blockchain technology provides security for the transacting data whereas it does not guarantee any security against a particular account. An additional concern could be the execution of this new technology along with legacy systems, along with maintenance and improvisation of parameters such as scalability and accountability.

Smart contract risks:

Business processes, legal, and other financial details are bound to the blockchain, which depends on the external Oracle base for its operation. Therefore, any attack on the Oracle base will be a significant issue.

Value transfer risks:

The major property of blockchain technology is that there is no central authority, and the architecture is decentralized; therefore, the transfer of value can be done among different peers without any hindrance. These risks need to be efficiently managed to harness the advantage of blockchain technology.

2.3 Solution Direction

Based on the existing literature review and their solution, it is identified that a dynamic model of privacy that provides a pattern of computing data transaction process as expected by nodes designated for data acquisition (collection), storage, and remote monitoring using appropriate blockchain technology has not been considered in decision making for ethical disclosure of private data in the smart home digital healthcare ecosystem. This assessment is based on the analysis of various data security and privacy concerns arising from the need to limit the transparency of sensitive data in transit to only authorised parties through a model that dictates the actions of data publishers and grants due access to data subscribers on a need-to-know basis.

Therefore, the motive of this review paper is to suggest a solution direction where an authorisation framework can be applied to ensure ethical disclosure of private data in a smart home installed with digital healthcare IoT that collects and send data over the air. The emphasis of ethical disclosure is on the transparency of use (purpose) of the collected private data to guarantee both data confidentiality and user privacy. The framework is broken down into the following dimensions:

- approach for securing private data against threat model,
- architecture of approach,
- privacy model for decision-making in Blockchain implementation,
- performance evaluation of the approach towards privacy preservation.

Ethical usage of data should be factored into privacy and security discussions, more so, when data generated data needs to be protected because it is IoT's true value in the scenario of smart home application. Ethical concern on privacy preservation based on the consent of home residents (i.e., data subject) is encapsulated in the smart contracts to implement, as this will grant due permission to the use of the data based on the purpose of use. The compliance with the purpose of use, the purpose of use, and the use pattern will be visible and transparent to all stakeholders through the traceability feature of the utilised blockchain, the consensus algorithm, and the smart contracts deployed. Informed consent and acceptance of the data/information to collect, store, monitor, and share among parties (i.e., data subscriber or consumers) are determined by the publisher-subscriber model of smart contract, and access to the data request is granted based on the role of each participating nodes, concerning the data to share, whom to share with, the tenure of sharing, reasons/when to opt-out or stop sharing; and what to remain secret. Hence, this brings the concept of privacy and secrecy under one umbrella, the umbrella of smart contracts, to support emerging techniques for data ownership, sovereignty, and provenance required to promote the adoption of blockchain in domains such as healthcare.

However, some concepts have suggested the use of Perfect Forward Secrecy [160] and Zero Knowledge Proof [277] in the privacy preservation of sensitive data, and the possibility of using smart contracts to achieve a similar feat when deployed as an authorisation protocol. In light of this comparison, Perfect Forward Secrecy (PFS) and Zero-Knowledge Proofs (ZKPs) are cryptographic principles used to enhance privacy and security, but they serve different purposes and operate in different ways. In Table 11 are some key differences and their relationship with smart contracts in terms of privacy preservation and authorization protocols:

Table 11

Differences and relationship between PFS, ZKP, and Smart Contract

Perfect Forward Secrecy (PFS)	Zero Knowledge Proofs (ZKP)
<ul style="list-style-type: none"> - Refers to protocols where compromise of a session key does not compromise past or future session keys. For instance, it ensures that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. Essentially, even if an attacker gains access to the server's private key, they cannot decrypt past communications. - Typically uses ephemeral key exchanges to derive unique keys per session. - Protects past encrypted data even if long-term keys are compromised. <p>- Does not hide metadata like who is communicating</p> <p>Usage Scenario: commonly used in secure communication protocols(Sadhukhan), including those used for secure web browsing, emails, and messaging.</p>	<ul style="list-style-type: none"> - Allow one party (prover) to prove knowledge of some information to another party (verifier) without revealing the actual information, i.e., beyond the fact that the statement is true. The 'zero-knowledge' aspect refers to the fact that the verifier gains no knowledge about the aspects of the statement, except that it is true. - Uses cryptographic methods to essentially "encrypt" the sensitive data into a proof. - Can be used to preserve the privacy of all data, not just exchanges. <p>- Hide metadata as well as data contents.</p> <p>Usage Scenario: ZKPs are used in various applications, including authentication systems and blockchain transactions (Kayvan/Jims), to preserve privacy. E.g., Zcash, a cryptocurrency, uses ZKPs to allow users to verify transactions without revealing any information about the amount, the sender, or the recipient.</p>
Smart Contracts as an Authorisation Protocol:	
<ul style="list-style-type: none"> - PFS could be implemented by deriving session keys on-chain from ephemeral key pairs. - PFS protects past communications - Smart contracts are one way to achieve PFS - While smart contracts can enforce certain aspects of key management, the typical use case for PFS is in the transmission of data, which is a function more closely associated with communication protocols than with smart contracts. 	<ul style="list-style-type: none"> - ZKP is better suited to prove identities and credentials in zero knowledge. - ZKP allows selectively revealing information like access rights, without exposing entire user profiles or transactions. - ZKP can hide all sensitive data - ZKP methods are better suited for fully private authorization - Smart contracts can be written to conduct certain types of ZKP, especially on blockchains that support more complex cryptographic operations. This is particularly relevant for privacy-preserving blockchains or for conducting confidential transactions.
<ul style="list-style-type: none"> - Functionality: Smart contracts are self-executing contracts with the terms directly written into code and stored on the blockchain. They automatically execute actions when predefined conditions are met, without requiring intermediaries. - Suitability: Smart contracts could be used to facilitate or enforce privacy-preserving mechanisms by stipulating those certain protocols or methods be used within transactions. However, the smart contract itself is not what provides PFS or ZKPs, rather it would be the cryptographic methods that the smart contract stipulates or enforces. - In essence, while PFS and ZKPs are cryptographic mechanisms for securing data and ensuring privacy, smart contracts serve as facilitators or enforcers of predefined rules. Smart contracts can be designed to integrate or interact with PFS and ZKPs by embedding these conditions into their code, thus leveraging the benefits of these cryptographic principles in a decentralized and transparent manner. However, the implementation of such features requires a deep understanding of cryptography, as well as a blockchain platform that supports these complex operations. 	

The features and functionality of the suggested smart contract and permissioned BC-based architecture depicted in Fig. 22 are capable of tackling certain challenges in healthcare applications such as in data confidentiality, sharing, usability, interoperability, and real-time medical data updates; thereby delivering

improved secure data management and privacy preservation scheme. A similar approach implemented in [278] utilised Hyperledger Fabric to securely and scalably manage data acquisition, storage, and monitoring process of home residents' sensitive data to preserve their privacy, deliver efficient permission management among stakeholders for enhancing collaborative clinical decision support and comprehensive continuum of care via the smart home system.

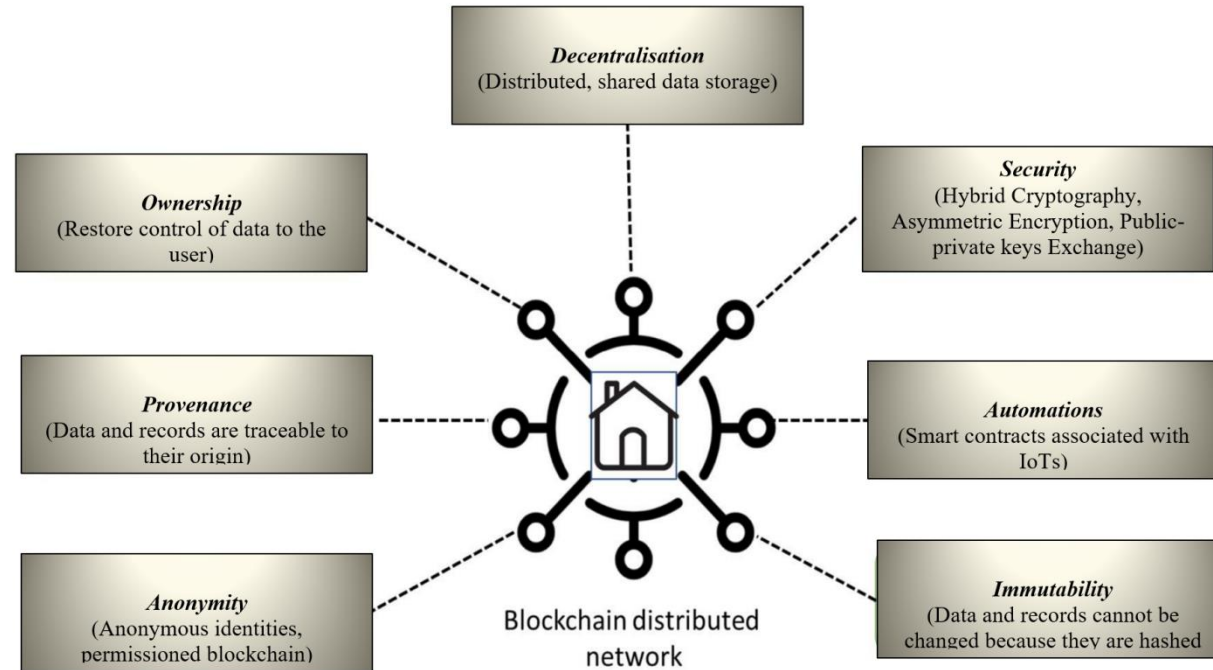


Fig. 22. Identifiable features of blockchain for improved privacy preservation in a smart home healthcare system.

The proposed solution addresses concerns in the areas of:

- Acquisition of data from residents, monitoring, and intervention at home using IoT devices.
- Decentralized data management and storage to avoid data manipulation issues, mistrust among network participants, and SPOF.
- Privacy and security aspects of the overall smart home ecosystem during the cross-continuum of care.

The solution strategies of this paper are summarized as follows:

- At first, this research introduces a user-centric **interoperable** authorisation framework that allows residents to have control over data management processes in a smart home's healthcare scenario to maintain the security, privacy, and integrity of their well-being data. This framework could utilise Hyperledger fabrics, private

Ethereum, or blockchain implementation using the PoA consensus algorithm as a decentralised data distribution technique. Moreover, permissioned distributed ledger solutions can as well utilise Hyperledger composer and store well-being data in IPFS to achieve scalability in the proposed private blockchain network. The decentralization feature of this framework ensures no SPOF, transparency of data usage, and integrity of data along its value chain of transaction within the participating nodes.

ii). The well-being transactions are hashed, encrypted, and stored on the IPFS off-chain storage, while the location of the storage in the IPFS is turned into hashes to compose blocks. Such blocks follow and are linked to each other sequentially in what can be described as a chain of blocks - blockchain. Moreover, the IPFS is a form of a distributed hash table (DHT) used to maintain the scalability efficiency, and integrity of the Blockchain. IPFS (InterPlanetary File System) and blockchain both offer decentralized storage solutions, but they differ in their fundamental design, purpose, and storage patterns. Below (Table 12) is a descriptive analysis of the storage management, retrieval, and transfer distinctions between IPFS (often used for off-chain storage) and blockchain (on-chain storage)

Table 12

Storage distinctions between IPFS and blockchain

Criteria	Blockchain (On-chain)	IPFS (Off-chain)
Purpose and Design	<ul style="list-style-type: none"> - Primarily designed to create an immutable ledger of transactions. - Ensures data integrity and authenticity through cryptographic means. - Utilizes consensus algorithms to validate and agree upon the state of data across nodes. 	<ul style="list-style-type: none"> - A peer-to-peer distributed file system designed to make the web faster, safer, and more open. - Focuses on content-addressable storage, where data is retrieved by its hash rather than its location. - Does not have a built-in consensus mechanism like blockchain
Storage Patterns	<ul style="list-style-type: none"> - Data is stored in blocks, linked together cryptographically to form a chain. - Every node on the network stores a complete copy of the blockchain, making it highly redundant. - Due to redundancy and the need for consensus, on-chain storage is expensive and slow, making it unsuitable for large files or high volumes of data. - Data stored on the blockchain is immutable; once recorded, it cannot be altered or deleted 	<ul style="list-style-type: none"> - Data is broken into blocks, and each block is addressed by its cryptographic hash. - Nodes store only the content they're interested in, plus some indexing information to help locate data. - Data retrieval is done using its hash, allowing for faster, peer-to-peer data fetching, ideal for large files or data sets.
Immutability and Persistence	<ul style="list-style-type: none"> - High durability and persistence due to the distributed and redundant nature of the network. 	<p>While the content-addressing ensures that the data has not been tampered with, there is no inherent guarantee of data persistence. If no node on the network holds a piece of data, it could be lost.</p> <p>Systems like Filecoin aim to incentivise storage on IPFS, thereby providing more durability guarantees.</p>

	- Blockchain's expensive on-chain storage costs often lead implementers to store only essential transaction data on-chain.
Usage in Combination	<ul style="list-style-type: none"> - For larger datasets or files (like images, documents, etc.), a common pattern is to store the data on IPFS and then store the IPFS hash of that data on the blockchain. - This provides a balance between the immutability and authenticity guarantees of the blockchain and the more efficient and scalable storage of IPFS.

Therefore, while both blockchain and IPFS offer decentralized solutions, their storage patterns and use cases differ significantly. Blockchain excels at creating an immutable record of transactions, while IPFS offers a more scalable solution for storing and retrieving larger datasets or files.

iii). The design emphasizes a user-centric approach with data ownership and provenance where the data subject (home resident) has complete access control over their data, and grants access permissions to the authorized stakeholders. Access-right to transactional data is based on smart contracts that encapsulate agreements inculcating deontological normative ethical regulation to derive an acceptable consent with proof of acceptance from data subject for data sharing and monitoring, leading to more resilient systems against data interception or leakage.

Hence, this study introduces an authorisation framework that exploits features of blockchain to ensure IoT data access protection vis-à-vis user's privacy during the well-being monitoring process where physiological and environmental data in a smart home are securely managed.

3. The Solution Methodology

Providing the requisite solution to challenges faced that could warrant adopting emerging technologies such as blockchain, cryptographic, AI-based, and authorisation schemes in the IoT ecosystem is majorly influenced by the scenario and the prioritization of security concerns to alleviate. Managing trade-offs encountered when certain evaluation metrics are put in place to achieve significant security and privacy benefits is of utmost importance and the focus of this paper. Moreover, the evolution pathway of smart home concepts in [7] is vast, and to secure the related technologies and services in this pathway, e.g., in smart healthcare, this paper presents a “privacy-by-design” procedure to achieve an authorisation scheme through a framework, and thereby complement earlier work cited, including several others who have utilised blockchain-based approaches for securing transactional information systems.

3.1. System Development Approach

This proposed tactic suggests an emerging research method that is applicable and could further interpret existing methods. The solution approach complements scientific theories, concepts, and models on how to protect data management processes in smart home systems, identify the components responsible for collecting, storing, and sharing sensitive data of residents, and devise means to ensure the confidentiality of data and user's privacy is preserved. Hence, a data ownership and access control scheme are functional requirements. To design a requisite framework of lightweight key exchange and access control systems, an agile prototyping approach with iterative processes consisting of *prototyping-feedback-improvement* modules is considered to reach the basic goal of providing

overall system functionality. Stages include Planning, Analysis, Design, Deployment, and Implementation with mnemonic ‘PADDI’. In this design process, end-user participation is needed to determine the desired level of privacy preservation. The methodology of this research contains:

- 1). Introduction of suitable lightweight transport encryption among nodes responsible for data acquisition, storage, and monitoring on the private blockchain implementing a PoA consensus algorithm.
- 2). Derivation of a privacy model to design an authorization framework.
- 3). Design of a publisher-subscriber smart contract for fine-grained access control.

3.2. Defining the Scenario

To proffer a solution to the unresolved diverse issues of data protection and user privacy in IoT-enabled homes, a potential case study scenario of a smart home with a digital healthcare facility installed to remotely monitor and offer instant/prompt care assistance to occupants (also referred to as smart home healthcare system) is specified to adequately identify the needed components and processes. Such a home is equipped with numerous connected wearables and nearables, i.e., activity and environmental sensors to remotely monitor the well-being of an elderly resident. Wearables such as smartwatches are used to track all key health metrics [279] and allow continuous collection and recording of the data streams of physiological parameters, i.e., movement of occupants, and relevant environmental variables [280].

In essence, the datasets of interest are typically described as follows:

- Element: The data subject being monitored (on which data are collected, and stored), a resident or inhabitant smart home; IPFS and eHealth Expert System.
- Variable: An attribute/characteristic of interest for the element e.g., lifestyle or well-being data.
- Observation: The set of measurements defining collected data for a particular element e.g., Set of Personal Activity Data (SoPAD) and Environmental Data (ED) being collected and exchanged between authorized parties i.e., healthcare providers (i.e., doctors, hospitals, pharmacies, laboratories, health insurance companies, etc.)

IoT devices collect, share data and resources; act and react to environmental changes, with or without human intervention. Therefore, discriminatory disclosure and use of the resident’s information is possible. Data leakage of their well-being status during the process of data acquisition, monitoring, or storage should be prevented. Thus, the solution direction is tailored to resolve the following research questions:

Q4: How can the monitored resident ensure that their set of personal sensitive data and data collected from their private environment sent outside their home is only accessed by authorized parties (e.g., authorised storage nodes and a stack of carers in the monitoring nodes) and that sensitive data is not altered for any maliciously by a third party?

Illegitimate collection of smart home users’ sensitive (health) data comes under questioning and is to be addressed alongside safeguarding and securely sharing the home user’s data with healthcare providers (i.e., doctors, hospitals, pharmacies, laboratories, health insurance companies, etc.)

Q5: How can the transparency of the use of the data collection be ascertainable, and made beneficial to the data owner in terms of service delivery i.e., care offered and received?

The purpose of collection of the monitored data should be justified through a transparent process that reveals the use of the data including the processing techniques,

disclosure terms, who the data subscribers are and their usage pattern, and the benefit of sharing such sensitive information to the data owner.

The direction to follow in proffering a solution to this problem is to protect the data acquisition process, and the location where the collected data is stored, provide shared transparency of data processes and define entities with an acceptable authorisation that can subscribe to and use the data through a contractual agreement i.e., smart contracts.

3.3. Framework Description

To handle issues relating to deprivation of privacy, all stages of the data value chain are considered, including acquisition/collection, storage, processing, and use. In addition, two possible solutions by practice, namely: privacy by design, and privacy-enhancing technologies [135] are investigated. The former is a concept that takes place before the development of a product or service and signifies the integration of privacy protection into both technology (devices, networking platforms, etc.) and regulatory policies (privacy impact assessments); while the latter permits embedding enhanced privacy technologies to avoid personal data compromise, rebuild trust among users and service providers. To this effect, a dynamic model of privacy that provides a pattern of computing data transaction process as expected by nodes designated for data acquisition (collection), storage, and remote monitoring using permissioned PoA-based blockchain technology will be employed in decision making for ethical disclosure of private data in the smart home digital healthcare ecosystem. The hierarchical structure and distributed trust mechanism considered with this approach are viable solutions that could maintain blockchain compatibility with the specific requirement of IoT for the provision of data security and users' privacy in the context of smart homes. In essence, the framework is viewed from three interrelated dimensions (Table 13).

Firstly, through an architecture that defines the composition of the role-based peer-to-peer logical network of participating nodes, implementation techniques of the lightweight hybrid encryption scheme, the data distribution technique of the PoA-based blockchain, and execution of authorisation protocol.

Secondly, deploy an approach for scalable storage technique that supports ethical disclosure of sensitive data. Using IPFS/blockchain is a means of utilising the synergy of these two technologies to handle large amounts of sensitive data in a secure, transparent, and efficient manner that reduces redundancy and ensures data availability. To ensure controlled disclosure, otherwise referred to as ethical disclosure, smart contracts on the blockchain can govern who has access to the data stored on IPFS. This way, the disclosure of sensitive data is controlled and automated, and the permissions can be transparently verified on the blockchain. Transparency of the use of data is evaluated with a decision-making model for privacy designed for the proposed blockchain implementation that uses an authorisation-based consensus algorithm (PoA).

Lastly, an approach for performance and threat evaluation to prove the resilience of the proposed authorisation scheme is introduced. Thus, the proposed authorisation framework classification aims to ensure the ethical disclosure of the private data of a smart homeowner using BCoT is depicted in Fig. 23 and described as follows:

Table 13

Inter-related dimensions of the proposed authorisation framework

Security Features	Technique	Benefit
The architecture of the approach	-Node Composition: Publisher, Subscriber and Client Nodes -Lightweight hybrid encryption scheme between nodes. ECES mode of ESDSA/ECDH and AES-EAX -PoA-based blockchain data distribution technique	-Logical connection of nodes based on role i.e., the home gateway is the data publisher, while the IPFS and monitoring node are data subscribers. -Efficient transport encryption of sensitive data transaction data between publisher and subscriber nodes using secure hashing, and digital signature for data authentication and verification. -Pre-authentication of nodes, selection of validating nodes based on trustworthiness. E.g., for the encrypted sensitive data stored on the blockchain, access to the decryption key can be limited to the authorised nodes only based on the implemented privacy model.
	-Permissioned BC Technology (On-chain DB Storage) -Inter Planetary File System IPFS (Off-chain DB Storage) -Smart Contracts	- Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. - Makes blockchain suitable for the recording of events, medical records, and other records management activities, such as identity management, transaction processing, documenting provenance, etc. - Content-addressed storage model, which means the content itself is addressed by the hash of the file, making the network more efficient, secure, and decentralized. - Each file and all the blocks within it are given a unique fingerprint called a cryptographic hash. - Controlled disclosure of sensitive data based on e-consent authorisation, on top of the blockchain to govern who has access to the data stored on IPFS.
Approach for scalable data storage and fine-grained access control		
Approach for performance and threat evaluation	Performance - Evaluation Metrics (latency, time, energy) Resilience Testing – Shellcode injection Privacy Assessment - LINDDUN and STRIDE	-To determine the overheads that could delay the response time to secure data in transit. -To determine the performance to detect and respond to interception threat. - To utilise LINDDUN's six steps which provide a systematic approach to privacy assessment. - Evaluate resilience to know threats using the STRIDE mnemonic

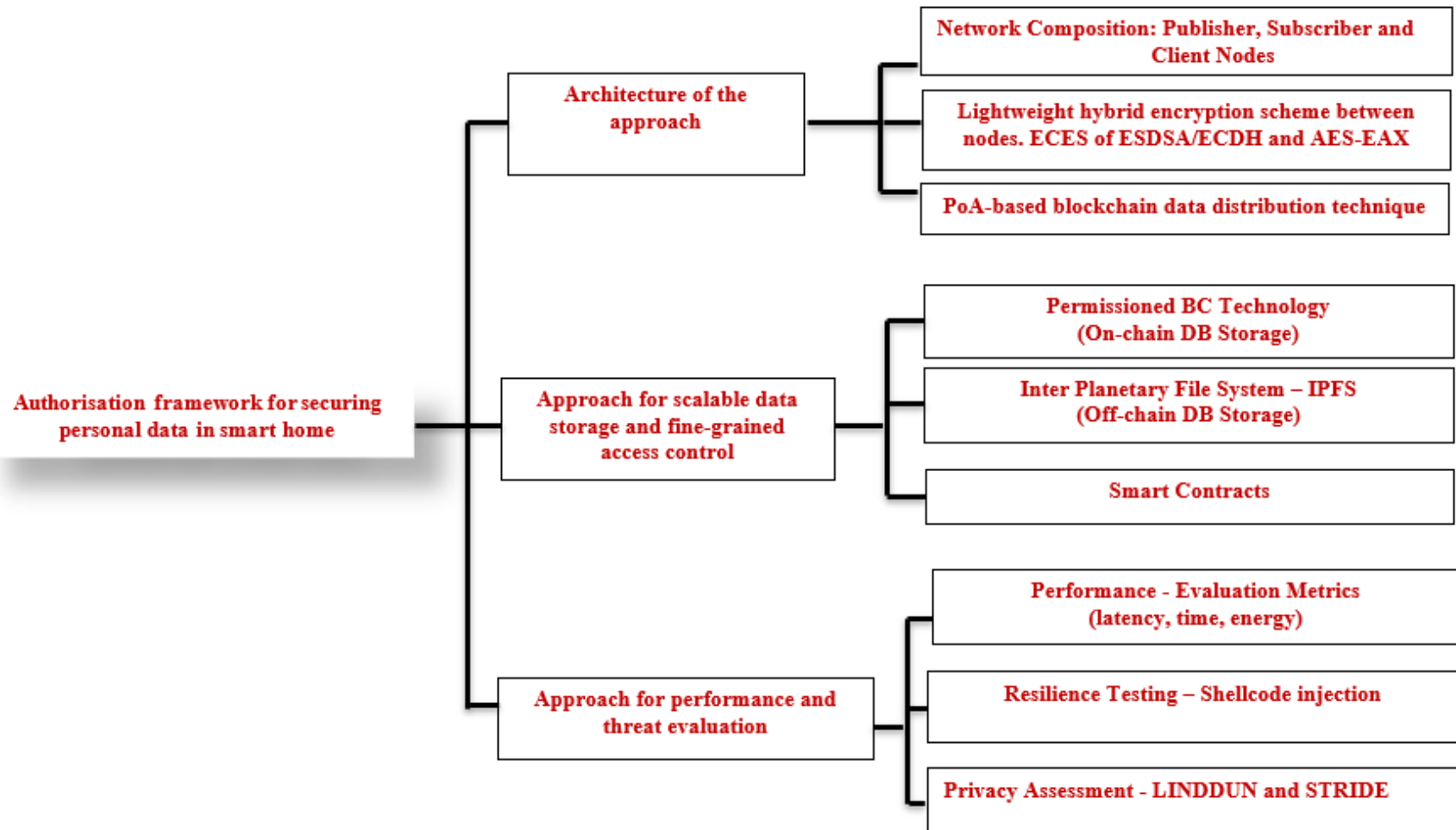


Fig. 23. Authorisation framework classification for ethical disclosure of personal data in a smart home healthcare ecosystem using smart contract-based blockchain.

3.3.1 On the Architecture of Approach

The network topology of the smart home healthcare ecosystem is designed based on a data publisher-subscriber model (Fig. 24). A logical network of peer-to-peer nodes is established for the PoA-based blockchain network where a hybrid cryptography scheme is applied for secure data exchange, and a reputation-based consensus algorithm for the distribution of personal data transaction among the nodes on the blockchain. The arrangement of the BC is such that:

- The 3 Nodes have a copy of the ledger of blocks.
- Data transactions within the blocks are encrypted with complex algorithms.
- Secure transport of P2P transactions through lightweight encryption key exchange.
- Unauthorized Node(s) are unable to intercept or alter data.

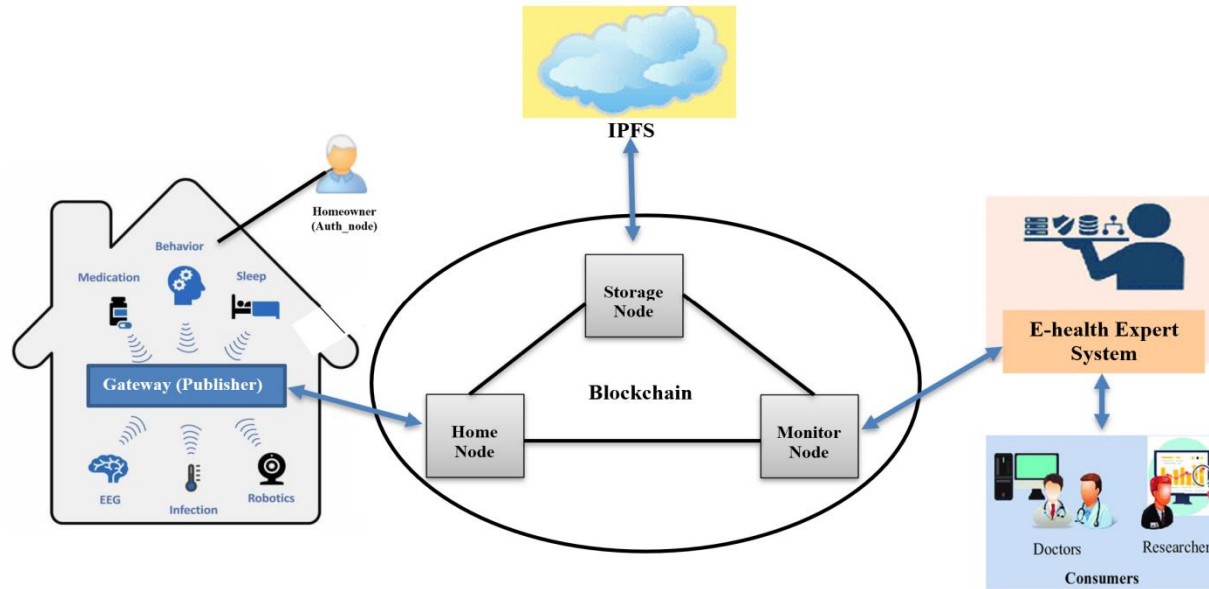


Fig. 24. A layout of BC in smart home healthcare service delivery identifying the gateway to the Blockchain, the owners (data subject), and the authorized subscribers (e-health and storage nodes) to access the private data.

3.3.1.1 Network Composition

The overview of the proposed smart home ecosystem and the setup of the BCN are duly discussed. As illustrated in Fig. 25, the three nodes describing the smart home healthcare scenario considered in this study are as follows:

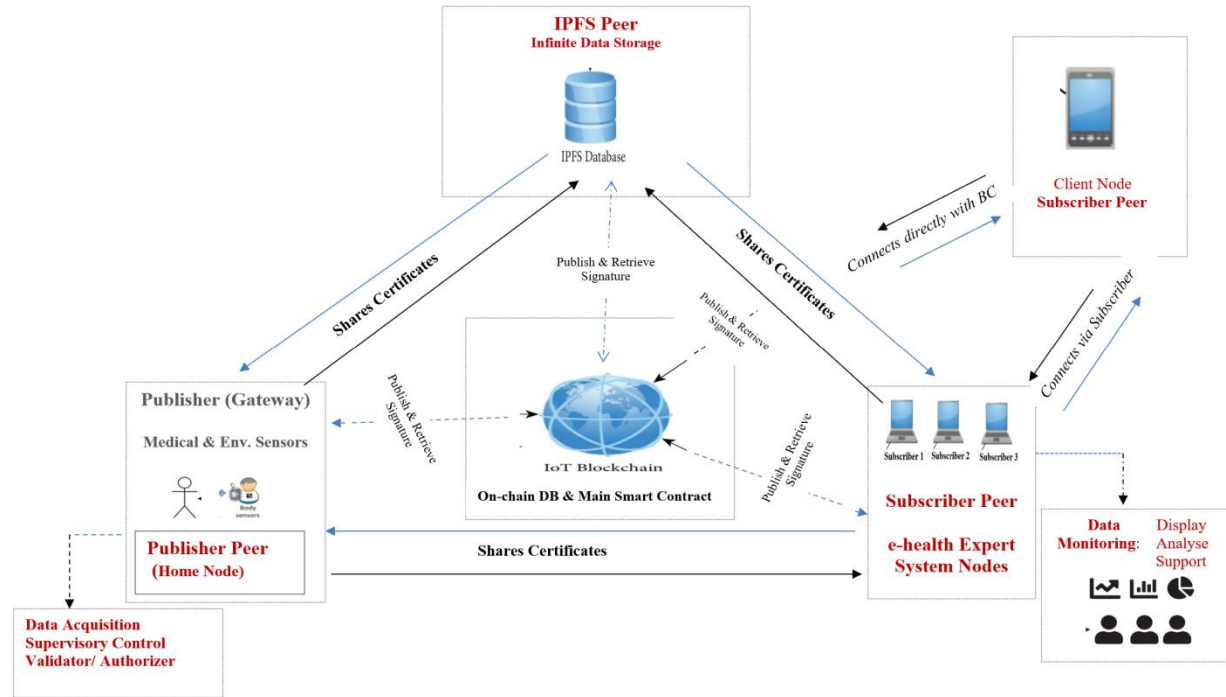


Fig. 25. Authorisation Framework made up of Nodes (Home Gateway- Publisher; IPFS, Client Node, and e-Health Expert System - Subscribers)

(i) Smart Home (Publisher Node): - contains low-end IoT Devices i.e., wearable sensors for remote health monitoring [281] and environmental sensors, that generate infinite data within the smart home. The home gateway, a high-end IoT device aggregates all data collected and publishes the data to the permission BCN. This setup is to overcome the network constraint of connected objects (low-end IoTs) in a smart home not able to directly connect to the BCN due to their limited processing capacity and energy power. Thus, the introduction of an intermediary high-end edge category of IoT [251], called the gateway connects the smart home to the BC. The data owners, the monitored elderly persons living in smart homes can access this data as well.

These individuals would have specified earlier on through an e-consent a set of authorised persons or organisation permitted to access their data. Table 14 illustrates the IoT devices to use in the data acquisition process and information stakeholders (actors).

Table 14

Smart home actors and data collection process

Actors	Description	Datatypes			
		SoPAD		ED	
		Symptoms Monitored	Sensor	Ambient Monitored	Sensor
Data subject – Elderly homeowner	in <i>SH</i> whose PII (well-being data) is to be selectively disclosed, a fully trusted entity and owns a PDA.	Body Composition e.g., BMI* & BMR*	BIA* Sensor	Temperature,	BMP280
Data Collectors	low- end IoT devices (sensors)	ECG*	Samsung Watch4	Pressure	
Data Publishers	High-end IoT nodes (HG, Rasp Pi4); semi-trusted	Movement	Samsung Watch4	Air Quality	MQ 135Gas Sensor
Data Subscribers	Requester(s) of home data; semi-trusted	Heartbeat Rate	Samsung Watch4	Humidity	Envi & AQ RaspPi
Smart Contracts	Defines authorisation policies among participants for fine-grained access control	Gait Appraisal	Samsung Watch4	Air Quality Camera	Rasp Pi Camera Module V2.1.
Consensus participants	Nodes on the BCN: Home Gateway (HG), IPFS, eHealth Expert Stack, Clients (Apps)				

Legend

- *BMI Body Mass Index
- *BMR Basal Metabolic Rate
- *BIA Bioelectrical Impedance Analysis
- *ECG Electrocardiogram

A major contribution of this study borders around the non-transparency of the use of collected private data, which becomes an ethical concern when the purpose of usage is undefined, and the subscribers/consumers of such data are unknown. Therefore, mechanisms that allow data owners to monitor who has access to their data and to regulate who has this access are paramount. The privacy scheme and transparency features of permission blockchain are more of a centralised approach to data management rather than decentralised, and therefore be seen to be counterintuitive. However, the transparency of data management processes is of utmost importance in this scenario. A meaningful disclosure comes with a desired level of access control that permits as much data as is needed to authorised parties only. In such a way, the user's private data is adequately preserved while necessary information is revealed to data subscribers, a win-win situation for the data owner. Similarly, data anonymity could conceal the identity of the data owner, meaning the confidentiality of personal data, when anonymised, is equally a justifiable means of preserving the privacy of user data. However, the application of statistical models in emerging studies has revealed how relatively easy it is to reidentify an individual from a supposedly anonymised dataset, even when such datasets are incomplete [282].

Ethics is of concern when personal data are collected and are to be protected to avoid non-transparency of how they are used. Privacy is the option to limit the access others have to the data owner's information e.g., on PII. The question is, what happens if the confidentiality of private data in a smart home system

cannot be guaranteed? Private data may be under the threat of interception without the knowledge of the smart home user (i.e., device, communication, storage, and services could become compromised). Confidentiality is the specific security requirement considered in addressing the data security and user privacy concerns in our scenario.

Thus, smart contracts application to such a scenario extends and leverages BC solution earlier introduced i.e., contracts are hosted on the Blockchain. The contract is a collection of code and data (occasionally referred to as functions and state) which is deployed using cryptographically signed transactions on the BCN; and is/are executed by nodes within the BCN. All nodes that execute the smart contract are expected to derive the same results from the execution, and the results of execution are recorded on the blockchain [33]. In defining the requisite access control technique for this smart home healthcare ecosystem which includes specifying the formal relation between data owners and data subscribers, smart contracts are considered as the cornerstone of the proposed BCoT architecture. Consequently, three types of contracts are defined for this scenario.

(ii). Off-chain database storage (Storage Node): - is the **distributed storage service provider for infinite data** with an efficient and similar storage schema relational to Blockchain data storage scheme, and as a peer connection on the permission BCN. However, the storage node can also be identified as a data subscriber.

(iii). eHealth Expert System (Subscriber Node): – This peer represents caregivers and affiliates that subscribe to the smart home data publisher and IPFS to monitor private data. Examples of actors in this domain include clinicians, therapists, pharmacies, health insurance agencies, relatives, and any other party granted permission to access the data publisher directly or query IPFS storage for data. This subscriber node(s) is also a node on the permission BCN and is pre-authenticated. The subscriber's smart contract defines the access level privilege a particular data subscriber is authorised with. **Electronic health (eHealth) comprises the fields of telemedicine, eHealth in prevention, health promotion and care, eHealth and economics, digitalisation of information and content, and eHealth for research and health reporting [217]. Thus, the main fields of IT, telehealth, and health management are depicted in Fig. 26. The IT leverages blockchain for a secure business process management of data in the two other fields, making it a crucial component of the value chain of care rendered through the health sector [82, 83].**

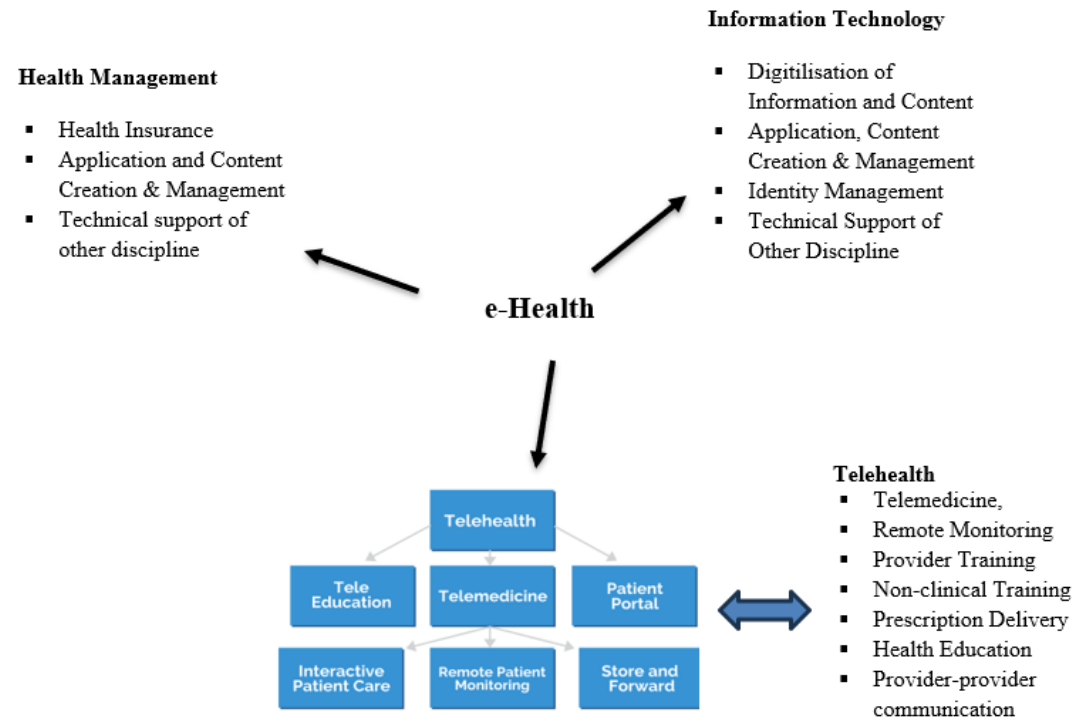


Fig. 26. Illustration of the fields of e-Health expert system, adapted [217]

(iv). Clients: – these are device or service applications connected to the subscriber nodes or directly to the permission BCN. Clients are subscribers as well participating in data requests and access transactions from both the sensors via the gateway, the off-chain, and on-chain storages.

3.3.1.2 Proposed Cryptography Scheme

Blockchain implementations leverage hybrid cryptography. The use of efficient transport encryption on sensitive data (i.e., SoPAD and ED) emanating from wearables to the home gateway is crucial in ensuring the integrity of the in-house data collection process. Moreover, lightweight hybrid encryption schemes are needed to guarantee the desired confidentiality, integrity, and availability of data in transit. Elliptic Curve Cryptography is well suited for this scenario as it provides a wide range of flexible and efficient encryption schemes for resource-constrained IoT environments. The elliptic curve integrated encryption scheme (ECIES) integrates ECC asymmetric and symmetric cryptography to ensure scalable transport encryption with minimal overheads. ECDSA of a reasonable key length can be used to generate key pairs and provide digital signatures for authentication and verification, ECDH to enable the secret key establishment through key agreement and derivation (e.g., HMAC-KDF, a hash-based message Authentication Code -key derivation function), and implement EAX(Encryption-Authenticate-Translate) or GCM (Galois Counter Mode) mode of AES, since these two modes are most preferred for the inherent authenticated encryption, confidentiality and integrity they provide. The combined use of ECC and AES allows for the security benefits of both public-key and symmetric encryption. ECC provides the secure key agreement, ensuring that even if an attacker observes the exchanged public keys, they cannot deduce the shared secret. Once the shared key is established, AES provides a fast, scalable, and efficient encryption of data. Fig. 27 illustrates the lightweight user authentication scheme [160] process logic for sending encrypted activity level data (gyroscope and accelerometer data) from a smartwatch to the home gateway (data publisher), in the presence of adversarial behavior i.e., the home is semi-trusted.

The need to protect the personal activity data (SoPAD) of the elderly is of interest for the following reasons:

- i). Fall Detection: Accelerometers are widely used for fall detection algorithms. Falls are a significant concern for elderly individuals and detecting them promptly is essential for their safety and well-being. Accelerometers can detect rapid changes in acceleration, which are indicative of a fall event.
- ii) Daily Living Activities: Accelerometers can help monitor the performance of daily living activities such as walking, climbing stairs, or sitting down. Understanding these activities is essential for assessing an individual's mobility and well-being.

To maximize data insights, a combination of both accelerometer and gyroscope data is often used. By integrating data from both types of sensors, a more comprehensive understanding of the elderly person's motion and activities can be obtained. For example:

- Accelerometer data can provide information about the intensity of physical activities, such as walking or climbing stairs.
- Gyroscope data can help assess gait quality, detect abnormalities in posture or balance, and identify potential risks of falling

Furthermore, integrated data from both sensors can enable more accurate activity recognition, improve fall detection algorithms, and provide a richer context for understanding the elderly person's movements and well-being. While gyroscopes are valuable for detecting rotational movements and can be useful for gait analysis in specific scenarios, they are not as directly relevant for general activity monitoring in a smart home setting.

In summary, for monitoring the well-being of the elderly in a smart home setting using a Samsung S4 watch as a wearable, the accelerometer data will provide more data insights and be more practical for activity recognition, fall detection, and overall activity monitoring.

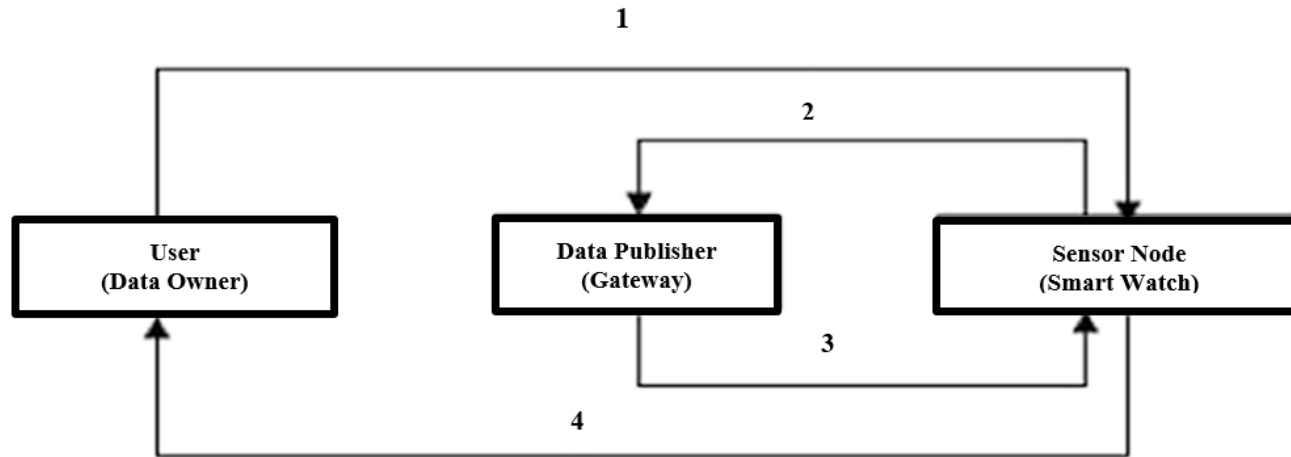


Fig. 27. Lightweight user authentication scheme for IoT using ECC.

Having ensured data transactions within the smart home, it is important to perform the same for the peer-to-peer data transfer among nodes on the blockchain network architecture. Aside from the ECC/AES key exchange and data encryption-decryption between the three specified nodes, the data stored on the blockchain can be encrypted to add a layer of privacy protection. Sensitive health data can be stored in encrypted form, and access to the decryption keys can be limited to authorized parties only. This is one of the several crucial roles a Proof of Authority (PoA)-based blockchain can play in providing an authorization framework for ethical disclosure of private data in the scenario of a smart home healthcare system for the well-being monitoring of an elderly person. This data encryption and privacy preservation technique decreases the likelihood of the information within records being accessible by unauthorized actors provided the private keys of BC network participants are not misplaced or compromised. Stolen, lost private keys or misplaced contract calls in permissionless blockchain used in cryptocurrencies such as Bitcoin, Ethereum, etc., have led to high-profile hacks in the blockchain systems [283, 284] where “Poly Network breach would be among biggest heists to target cryptocurrency industry”. However, due to the traceability and transparency feature in blockchain, reversal of the stolen asset was possible after security researchers said they had identified a trail of digital clues left by the hackers. In addition, SlowMist, a blockchain security firm, confirmed it managed to identify “the attacker’s mailbox, IP, and device fingerprints through on-chain and off-chain tracking” [285]. Due to the transparency of the blockchain and the use of blockchain analytics, laundering or cashing out stolen crypto assets is extremely difficult [286].

Consequently, newer blockchain networks are implementing creative measures to mitigate ongoing risk. In essence, the implementation of PoA-based BC is not entirely immune to consequences of loss of a private key or its compromise, only that the likelihood of occurrence is lower since all nodes are pre-

authenticated and validating nodes or approved accounts that approve transactions and create blocks are reputable, well-known to other nodes, and are trusted entities on the network. A grave repercussion in the case of loss of private key by the validators which they use to sign off on transactions and blocks is loss of trust. PoA-based BC effectiveness depends on the trust placed in its validators. If a validator's key is compromised, it could lead to a loss of trust in the network, as users may no longer believe in the validator's ability to secure their keys and, by extension, the network. In addition, the centralisation in PoA BC can create a single point of failure, and the loss or theft of a private key can be a significant systemic risk. On the flip side, the more centralised, permissioned nature of PoA blockchains may allow for swifter response and intervention in the case of a compromised key. The governing entities could potentially freeze the account associated with the lost or stolen key, or the network participants could agree to ignore or roll back fraudulent transactions, depending on the governance rules.

However, in permissioned blockchains, there might be advanced key management systems in place, with multi-signature protocols or hardware security modules (HSMs) to provide extra layers of security. These can prevent a single point of compromise from having system-wide effects. While the theft or loss of private keys is a security concern in both permissionless and permissioned blockchains, the nature of a PoA-based system creates unique challenges and opportunities. The more centralized control allows for rapid response but also places significant responsibility on validators to safeguard their private keys. As such, the security protocols, key management systems, and governance policies around key compromises are critical components of maintaining a secure PoA-based blockchain network.

The P2P PoA-based BCN proposes to employ an ECES hybrid encryption scheme more suitable for scalable data transactions i.e., in terms of the message size limitation observed in RSA when padding schemes (OAEP) are used with SHA256, to leverage on the deterministic and high rate of transaction in the PoA-based blockchain. Moreover, the deprecated use of 1024-bit RSA keys in 2010 by NIST due to an increase in computational power and advancements in cryptanalytic techniques, made the once-considered secure key length vulnerable to cryptographic attacks. Instead, the industry standard recommendation for security-sensitive applications is a transition to longer key lengths, such as RSA 2048-bit or the equivalent ECC 224-bit ECC to ensure a higher level of security against potential cryptographic attacks. For instance, some key considerations of RSA and ECC are:

- ECC relies on the elliptic curve discrete logarithm problem, which is mathematically harder than RSA's integer factorization problem. This allows ECC to achieve the same security with much shorter keys.
- A 192-bit ECC key has a strength of around 96 bits, compared to a 3072-bit RSA key which provides about 128 bits of strength.
- 96 bits and 128 bits are considered close enough in strength for most practical purposes.
- Recommendations often match a 192-bit ECC key with a 3072-bit RSA key as offering a comparable security level.
- NIST recommends both 3072-bit RSA and 192-bit ECC keys through 2030 for sensitive information.
- For even shorter ECC keys like 160-bit, a 2048-bit or 3072-bit RSA key is typically considered comparable.

Therefore, for a security level roughly equivalent to a 192-bit ECC key, RSA would need to use a significantly longer key size of around 3072 bits. The large RSA size required makes ECC more efficient for many use cases.

ECC (Elliptic Curve Cryptography) and AES (Advanced Encryption Standard) are two cryptographic primitives, which are typically used for public-key cryptography and symmetric encryption, respectively. In addition, AES encryption modes such as EAX, GCM, CBC, OFB, and CFB have been applied to complement ECC to provide a viable lightweight hybrid cryptographic solution in resource-constrained networks. However, the RSA limitation of having a maximum message size that can be encrypted especially when using SHA 256 with OAEP is often encountered especially in a situation where the smart home

healthcare ecosystem has numerous devices producing a large volume of data transactions. In practice, when aiming for "privacy by design" in transport encryption, GCM or EAX are block cipher schemes considered suitable and secure when implemented correctly since the two modes use similar security evaluation descriptors e.g., the underlying encryption mode, authentication mechanism, and nonce. The choice between them might be influenced by factors like performance, library support, and specific requirements of the application.

Choosing a key size for cryptography is of the utmost importance. The key length does not affect the encryption/decryption speed significantly. The performance is more dependent on the underlying processor performance. However, there are some points to consider regarding key lengths for transport encryption. Longer keys are more secure but slower. So, for instance, RSA 4096-bit keys are more secure than 2048-bit keys, but 2048-bit operations will be faster. For optimal security, transacting device keys should be equal. Using mismatched key lengths can potentially weaken security in some cases. For a 2048/4096 mismatch, the security level will be limited by the weaker 2048-bit client key. So, there is no real benefit in the server using a 4096-bit key. For client-server RSA encryption, typically the client encrypts data with the server's public key and the server decrypts with its private key. The client key length does not directly affect encryption/decryption speed in this flow. The server's private key length determines the decryption time. So, a 4096-bit server key will have slower decryption than a 2048-bit server key. In summary, the 2048 client / 2048 server will have faster performance than the 4096 client / 4096 server. 2048 client / 4096 server provides no real security benefit over 2048 client / 2048 server.

In [169], ECDSA with secp256k1 was implemented for the key pair generator, signature, and verification algorithm, and SHA 256 as a cryptographic hash function. The k1 curves are a specific class of Koblitz curves used in ECC implementation that have some special properties desirable for cryptographic implementations. But k1 variants have only been standardized for some key sizes. SECP256k1 - 256-bit Koblitz curve is of interest, and 256-bit ECC keys are considered special and widely used in cryptography for reasons such as:

- 256-bit is a sort of "sweet spot" for balancing security, performance, and interoperability.
- A 256-bit ECC key provides a very high-security level of around 128 bits of strength. This is sufficient security for the foreseeable future.
- 256-bit ECC keys are much faster in software than equivalent strength RSA keys (3072 bits or higher).
- 256-bit ECC is widely standardized and supported across platforms and protocols.
- The secp256r1 and secp256k1 curves were specially designed for optimal performance and security at 256 bits.
- secp256k1 is used extensively in Blockchain and cryptocurrencies like Bitcoin and Ethereum due to its speed and security.
- 256-bit security is the minimum recommended by NIST for US government applications beyond 2030.
- Going higher than 256-bit only provides marginal security improvements while impacting performance significantly.

In summary, 256-bit ECC combines versatility, performance, and future-proof security. It offers a balance suitable for a wide range of cryptographic applications. The standardization and special curves at 256-bit also make it efficient to implement. These advantages make 256-bit keys very popular for ECC across the industry.

SECP: SECP (Standards for Efficient Cryptography Group) provides standardised, secure, and interoperable elliptic curves that are optimised for the efficient implementation of public-key cryptography schemes like ECDSA and ECDH. SECP has the R1 and K1 variants.

- SECP curves are carefully chosen and vetted for cryptographic security and implementation efficiency.
- SECP256k1 uses a Koblitz curve. The discrete logarithm problem on Koblitz curves is theoretically harder, providing higher security.

- SECP256k1 is designed specifically for efficient high-security digital signatures, especially for Blockchain. It belongs to the SECP family of standardized curves by SECG.
- SECP256k1 has distinct mathematical properties optimized for digital signatures rather than encryption. SECP256k1 is defined over a 256-bit prime field.
- .- SECP256k1 provides strong security with 128 bits of strength. Comparable to 192-bit SECP or 224-bit prime field curves.
- So SECP256k1 has some specialized use cases, but SECP256r1 is meant for general elliptic curve cryptographic implementations such as in traditional cryptography or protocols like TLS.

The k1 curves are a specific class of Koblitz curves that have some special properties desirable for cryptographic implementations. But k1 variants have only been standardized for some key sizes. The relevant k1 curves are:

- SECP160k1 for 160-bit Koblitz curve.
- SECP192k1 for 192-bit Koblitz curve.
- SECP224k1 for 224-bit Koblitz curve.
- SECP256k1 for 256-bit Koblitz curve.

The r1 curves on the other hand are more general-purpose elliptic curves over prime fields. The r1 variants exist for more key sizes. Common SECP curves that are widely used for ECC include SECP160R1, SECP192R1, SECP224R1, SECP256R1, SECP384R1, and SECP521R1. The SECP curves are standardised and widely supported in cryptographic libraries and protocols like TLS, SSH, S/MIME, etc.

3.3.1.3. Distribution Technique

The implementation of a PoA consensus algorithm proposed does not require mining, therefore, high-performance nodes are not required to spend computational resources to solve complex mathematical puzzles as shown in Fig. 28. This consensus algorithm does not involve any form of mining incentives beyond rewarding nodes with access-right to transact data once the legitimate of the request is proven as defined in their associated contract based on their reputation and the efficient utilization of roles with the BCN. In addition, these characteristics in PoA provide a high transaction rate, high performance, and fault tolerance. Other benefits of PoA include:

- (i) The right to generate new blocks is awarded to a node with proven authority to do so and has passed a preliminary authentication.
 - Built-in identity attestation
- (ii) The interval of time at which new blocks are generated is predictable, i.e., performed in sequence at appointed time intervals by authorized nodes, leading to the increase in the speed at which transactions are validated.
 - POA Network can do up to 30,000 TPS with <3 second finality.
 - Higher transactions per second (tens of thousands of TPS)
 - Predictable block times (sub-second)
 - Transaction finality - blocks are deterministic, not probabilistic.

- (iii) tolerance to compromised and malicious nodes.
- (iv) Only selected trustworthy nodes known as validating nodes can generate new blocks, and their list is stored in the BC registry.
- (v) Validating nodes maintain the BCN (distributed ledger), and the order of nodes in the list of validators determines the sequence in which new blocks are generated by nodes.
- (vi) Energy consumption is far lower than mining-based chains.
 - Lower energy use without mining

Thus, PoA can offer higher performance and finality guarantees due to its permissioned nature and authority-based consensus. But there are centralization tradeoffs.

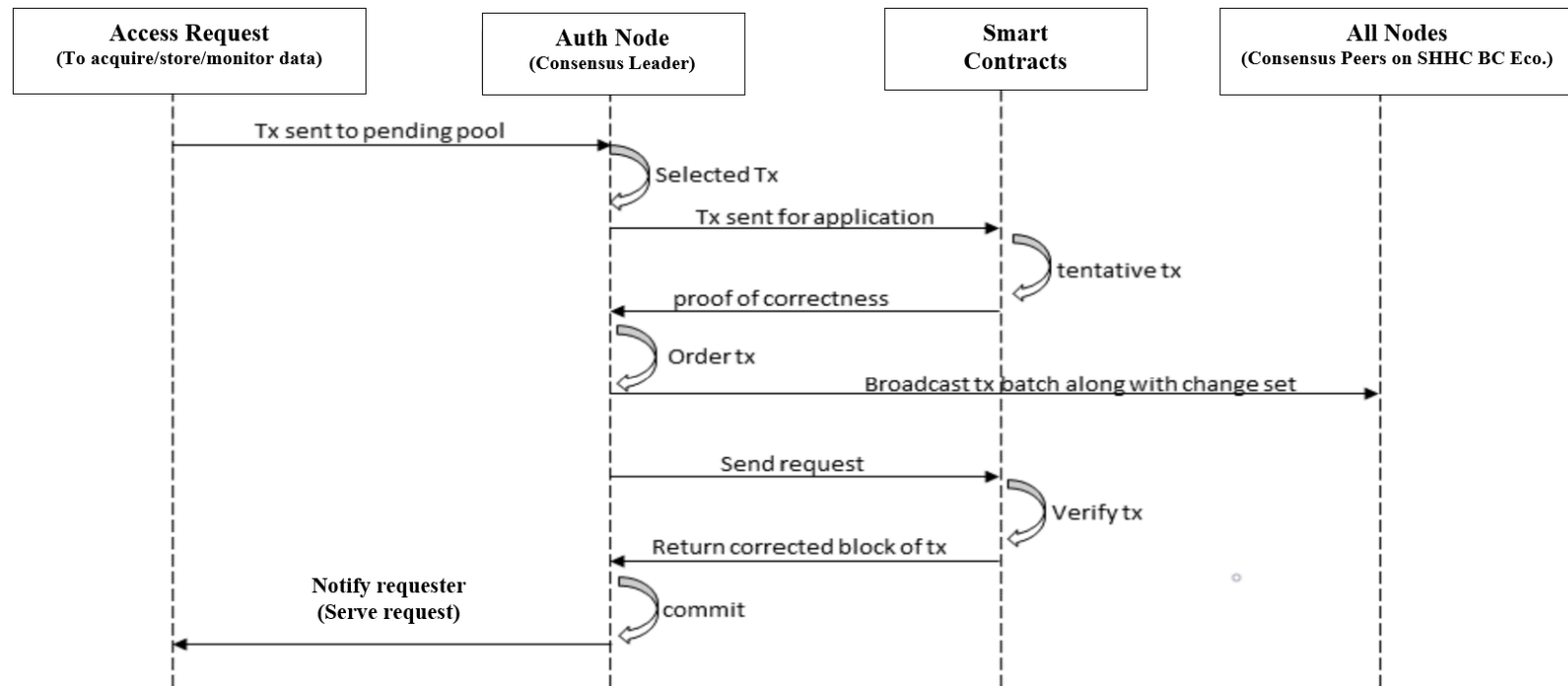


Fig. 28. Sequence diagram for the proposed PoA BCN in the smart home healthcare ecosystem

3.3.2 On the Approach for Scalable Data Storage and Fine-grained Access Control

Interception is a major threat to confidentiality, data privacy, and by extension an adversarial model that grants unauthorized access to an individual's private data. To ensure users' privacy in the smart home healthcare scenario presented, supervised authorisation is provided using a combination of secure and scalable data storage mechanisms, and role-based smart contracts (Table 15).

Table 15

Proposed data storage and access control mechanism for the smart home healthcare ecosystem

Technology	Description
Permissioned BC Technology (On-chain DB Storage)	<ul style="list-style-type: none">- Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.- Makes blockchain suitable for the recording of events, medical records, and other records management activities, such as identity management, transaction processing, documenting provenance, etc.
Inter Planetary File System – IPFS (Off-chain DB Storage)	<ul style="list-style-type: none">- Content-addressed storage model, which means the content itself is addressed by the hash of the file, making the network more efficient, secure, and decentralized.- Each file and all the blocks within it are given a unique fingerprint called a cryptographic hash.
Smart Contracts (Fine-grained access control)	<ul style="list-style-type: none">- Controlled disclosure of sensitive data based on e-consent authorisation, on top of the blockchain to govern who has access to the data stored on IPFS.

3.3.2.1 P2P Permissioned BCT (On-chain DB Storage)

In the permissioned BCN proposed, all nodes are pre-authenticated, which is like it is in a controlled corporate intranet, limiting participation to specific parties or nodes, and allowing for fine-grained controls [33]. This type of BCN is often deployed for a group of organizations and individuals, typically referred to as a consortium, and such is considered for the public eHealth expert system in this study.

3.3.2.2 Inter Planetary File System (off-chain DB Storage)

InterPlanetary File System (IPFS) is a P2P network for storing and sharing data in a distributed file system using a Distributed Hash Table (DHT) and is designed to work together with existing Blockchain protocols. Though not specifically built on Blockchain, it uses content-addressing to uniquely identify each file within the global namespace that connects IPFS hosts. These contents are accessible via peers located globally and can relay and store information. IPFS discover information using content address (identify content by what is in it) rather than the information location [287]. The basic principles of IPFS use the concept of unique identification through content addressing, content linkage using directed acyclic graphs (DAGs), and content discovery utilising distributed hash tables (DHTs).

The hash of the personal data storage location is kept on the BC while the actual encrypted data is stored off-chain on the IPFS decentralized storage. For instance, newly generated well-being data from any sensor (i.e., SoPAD) and those from the environment (i.e., ED) are occasionally forwarded through the publisher (gateway) to the IPFS (off-chain) storage. The gateway also broadcasts a message containing the hash pointing to the location of data stored on the IPFS to the

Blockchain (On-chain store). Thus, the IPFS is used as a secure decentralised data storage hub for sharing generated sensitive data emanating from a data subject in the smart home. This two-storage association is exploited to maintain the security and privacy of data collected within the smart healthcare ecosystem.

3.3.2.3 Smart Contract

This solution proposes the use of Smart Contracts to maintain rules, authentication, and communication between the different nodes and parties in the healthcare smart home system. Smart contracts are associated with each of the blockchain network participants to allow for fine-grained access control based on the management of private data in the smart home healthcare ecosystem. The smart contracts are described as follows:

(i). Publisher Contract Description: - This contract will first be specified before a user (his) subscribes to the system and connects their SH gateway to the BCN. Since all nodes in a permission BCN are pre-authenticated, a unique ID mapped to his blockchain address is received once the publisher contract is accepted. The list of the IoT devices to connect to the blockchain must also be specified using names for ease of access and identification of the generated data. In addition, the type of sharing mechanism to manage the publisher-subscriber association and the list of permissible addresses to access data i.e., addresses of authorised subscribers to the data, are to be specified.

The publisher's smart contract comprises the data subject's consent which allows any subscribing party to request a subset of or a full SoPAD and ED. This service allows the data subject to decide on how to react to requests, and which subsets of personal data they have agreed to share or want to share. The smart contract manages each request type of SoPAD/ED a data publisher provides to subscriber parties. The third party (subscriber) initializes contact with the publisher's smart contract once, requesting a certificate for future access to the SoPAD/ED. Upon the data subject's consent to the subscriber's request, an up-to-date SoPAD/ED can then be subsequently requested just in time whenever it is needed for processing.

The publisher smart contract provides the SoPAD/ED instantaneously once the certificate of the subscribing party is valid. Hence, it is no longer necessary to store the actual personal data of the subscriber.

(ii). Subscriber Contract Description: - This second contract should contain the address of the subscriber(s) in the blockchain, and the list of publishers to which it subscribes and should also state the specific list of sensors to subscribe to. The sensors are to be chosen by type, name, or the use of a wildcard to select all the available sensors associated with a certain publisher. This happens to be the critical component of the publisher-subscriber procedure since the generated data can be filtered before sending it to a subscriber based on the information recorded in this contract.

(iii). Client Contract Description: - The client contract is the third contract, serving as a mapping contract between normal nodes, or clients connected to the blockchain, and their respective subscriber contracts. The client's name is used here for ease of communicating with one another through a front-end application. This name is also mapped to the corresponding address in BC. For instance, the client connects to the IPFS node whenever it is requested by the end user, using the hash code to fetch the data generated by the sensor.

The proposed smart contract is expected to meet the following minimal requirements:

- The smart contracts are to have an interface that handles the initial request of a certificate for future requests of a SoPAD/ED.

- The smart contract should have access to a securely hosted decryption function, which will provide the function $Dec(X) = Enc(SoPAD/ED)$, where X is the element of $Enc(SoPAD/ED)$

The data owner is a single source that provides the smart contracts capable of decrypting the SoPAD/ED in question. This ensures they get a notification whenever SoPAD/ED is processed.

This functionality is handled by a BC functioning as an immutable access log. Described below is a model for the minimal interface for a smart contract to allow a subscriber to request a SoPAD/ED of the data subject and ensure they are notified whenever any of their SoPAD/ED is revealed to any subscriber.

- Request_Certificate (SubscriberID, Reason_For_Request)
- Request_SoPAD/ED (Certificate, Requested_Subset_Of_SoPAD/ED)
- Access to BC for $Dec(X)$, where X is the element of $Enc(SoPAD/ED)$
- Check_Verify_Of_Certificate (Certificate) checks if the requesting subscriber is allowed to be granted access to the SoPAD/ED based on the certificate provided with the request.

The data subject utilises the BCoT to ascertain high availability while maintaining full control over their data. To guarantee that copies of SoPAD/ED are up to date once the hash of SoPAD i.e., $H(SoPAD/ED)$ has changed, the timestamp in the SoPAD/ED can be modified whenever it is requested. This is simply because changing only the timestamp (without interfering with related personal data) results in a different hash forcing the subscriber to file a new request against the data publisher smart contract, should such a subscriber want to process an up-to-date SoPAD/ED. Thus, any processing of SoPAD/ED without the consent (or with prior request) of the data subject is easily identifiable because such a dataset is outdated. This mechanism assists in identifying subscribers who store personal data without the data subject's consent. Thus, for efficiency, the publisher smart contract could also inform the subscriber if a previous request of a SoPAD/ED is still up to date.

Therefore, to withdraw a once-given consent, changing the hash $H(SoPAD/ED)$ and invalidating the subscriber's certificate will suffice. Moreover, for every smart contract, a separate key pair is generated for security reasons, thereby making it possible to invalidate the public key supposing the private key for a particular SoPAD/ED is compromised. Fig. 29 illustrates the model of the publisher-subscriber contracts, with the workflow explanation.

a) Contracts with hardcoded participant address

```
//SPDX-License-Identifier: UNLICENSED
pragma solidity 0.8.19;

//publisher contract
contract publisherContract {
    //this is a variable that saves the publisher address
    address public publisher;

    //a mapping of authorized nodes. My thought is that this will contain addresses of the nodes participating in the blockchain
    mapping (address => bool) public authorizedNodes;

    //this maps addresses to the things some addresses can do(i.e functions to call/interact with)
    mapping (address => Permission) public permissions;

    //a variable to store the incoming ipfs hash
    string public dataHash;

    //a hardcoded example address for testing
    address public participant1 = 0x5838D6a701c568545dCfc803Fc8875f56beddC4;

    //a structure that defines permission types, whether to view or store data
    enum Permission {
        view_data,
        store_data
    } //manage_contract

    //events to monitor important occurrences(as defined by me)
    event hashUpdated(string indexed);
    event permissionGranted(address indexed);

    /*a constructor is executed once.
    this constructor should setup the authorized nodes,
    and give permissions to participating nodes
    */
    constructor() {
        authorizedNodes[participant1] = true;
        permissions[msg.sender] = Permission.store_data;
        permissions[participant1] = Permission.view_data;
        publisher = msg.sender;
    }

    //this function lets the publisher give view permission to other addresses
    function updatePermissionToView(address participant) public onlyPublisher {
        permissions[participant] = Permission.view_data;
        emit permissionGranted(participant);
    }

    //this address updates the hash from time to time. Only the latest hash is saved
    function updateHash(string memory newHash) public onlyPublisher hasPermissionToStore {
        dataHash = newHash;
        emit hashUpdated(newHash);
    }

    //a modifier is used to restrict some addresses from calling this function
    modifier onlyPublisher() {
        require(publisher == msg.sender);
        _;
    }

    modifier hasPermissionToStore() {
        require(permissions[msg.sender] == Permission.store_data);
        _;
    }
}

/*
this contract inherits from the publisher contract in order to access some important functions.
*/

contract subscriberContract is publisherContract {

    /*this is used to access the ipfs hash stored in the publisher contract.
    I have used the 'hasPermissionToView' modifier to introduce access control,
    so that addresses without permission cannot call this function
    */
    event dataRequested(address indexed, uint);

    function getDataHash() public hasPermissionToView returns(string memory) {
        emit dataRequested(msg.sender, block.timestamp);
        return dataHash;
    }

    //this is a function that returns the kind of permissions that an address has, whether to view or store data
    function checkPermissions() public view returns(Permission) {
        return permissions[msg.sender];
    }

    modifier hasPermissionToView() {
        require(permissions[msg.sender] == Permission.view_data);
        _;
    }
}
```

b) Contract with dynamic addition and verification of participants

```
// SPDX-License-Identifier: UNLICENSED
pragma solidity 0.8.19;

contract AccessControl {
    address public owner;
    mapping(address => bool) public authorizedNodes;
    mapping(address => uint8) private permissions;

    enum PermissionType { None, View, Store } // Added None for better permission management

    event PermissionUpdated(address indexed participant, PermissionType permission);
    event HashUpdated(string newHash);

    modifier onlyOwner() {
        require(msg.sender == owner, "Not contract owner");
        _;
    }

    modifier authorizedToStore() {
        require(PermissionType(permissions[msg.sender]) == PermissionType.Store, "Not authorized to store");
        _;
    }

    modifier authorizedToView() {
        require(PermissionType(permissions[msg.sender]) == PermissionType.View, "Not authorized to view");
        _;
    }

    constructor() {
        owner = msg.sender;
        // The owner of the contract has the ability to store data by default
        permissions[owner] = uint8(PermissionType.Store);
    }

    function setPermission(address participant, PermissionType permission) public onlyOwner {
        require(participant != address(0), "Invalid address");
        require(permission != PermissionType.None, "Invalid permission");

        permissions[participant] = uint8(permission);
        emit PermissionUpdated(participant, permission);
    }

    // New function to revoke permissions
    function revokePermission(address participant) public onlyOwner {
        require(participant != address(0), "Invalid address");

        permissions[participant] = uint8(PermissionType.None);
        emit PermissionUpdated(participant, PermissionType.None);
    }

    function getPermission(address participant) public view returns (PermissionType) {
        return PermissionType(permissions[participant]);
    }

    // ... other functions remain the same
}

contract DataContract is AccessControl {
    string private dataHash; // Data should be private and accessible only via function

    function updateDataHash(string memory newHash) public authorizedToStore {
        require(bytes(newHash).length > 0, "Data hash cannot be empty");
        dataHash = newHash;
        emit HashUpdated(newHash);
    }

    function getDataHash() public view authorizedToView returns (string memory) {
        return dataHash;
    }
}
```

Fig. 29. Model of the publisher-subscriber contracts

a) Contracts with hardcoded participant addresses:

This code defines two smart contracts, ``publisherContract`` and ``subscriberContract``, where ``subscriberContract`` inherits from ``publisherContract``. These contracts are meant to manage permissions for nodes in a blockchain network, specifically concerning viewing and storing healthcare data within a smart home healthcare ecosystem. The system is designed to ensure that data is ethically disclosed only to those entities that have the appropriate permissions. The breakdown is as follows:

1). ``publisherContract``:

- State Variables:

- ``publisher``: Stores the Ethereum address of the publisher (the entity that deploys the contract).
- ``authorisedNodes``: A mapping to keep track of which addresses (nodes) are authorized.
- ``permissions``: A mapping from addresses to their specific permissions. Permissions are represented as an enum, which can be either ``view_data`` or ``store_data``.
- ``dataHash``: A string that is meant to hold an IPFS hash, representing the location of data stored off-chain.
- ``participant1``: An example participant's address for testing purposes.

- Events:

- ``hashUpdated``: Triggered when the IPFS hash is updated.
- ``permissionGranted``: Triggered when permission is granted to a participant.

- constructor:

- Initializes the ``publisher`` with the address of the contract creator (``msg.sender``).
- Sets an example ``participant1`` as an authorized node and assigns permissions to the ``msg.sender`` and ``participant1``.

- Functions and Modifiers:

- ``updatePermissionToView``: Allows the publisher to grant an address permission to view data.
- ``updateHash``: Allows the publisher to update the ``dataHash`` variable (IPFS hash). This function can only be called by the publisher and the address with the ``store_data`` permission.
- ``onlyPublisher``: A modifier that restricts function access to only the publisher.
- ``hasPermissionToStore``: A modifier that checks if the message sender has permission to store data.

2). ``subscriberContract``:

This contract inherits from ``publisherContract`` and thus has access to its state variables, events, and functions.

- Event:

- ``dataRequested``: Triggered when data is requested, logging the requester's address and the timestamp.

- Functions and Modifiers:

- ``getDataHash``: Function that returns the current data hash; it checks if the message sender has the necessary permission to view data.
- ``checkPermissions``: Allows an address to check what permissions it has.
- ``hasPermissionToView``: A modifier that checks if the message sender has permission to view data.

An explanation of the workflow of the publisher-subscriber contracts is as follows:

- The publisher deploys the ``publisherContract``, and during deployment, the constructor sets the publisher's address and initializes permissions for the publisher and an example participant.
- The publisher can grant "view" permissions to other addresses using the ``updatePermissionToView`` function.
- The publisher can update the IPFS hash, which represents the healthcare data, using the ``updateHash`` function. This hash might refer to patient data, healthcare records, etc., stored securely on IPFS.
- Participants in the network can then interact with the ``subscriberContract`` to request the data hash (if they have view permissions) and check their permissions.
- Access control is enforced through modifiers, ensuring that only authorized participants can access specific functions based on their roles and permissions.

Security Considerations:

- The contract currently uses an example participant's address hardcoded into the contract, which is non-ideal for a production environment. Dynamic addition and verification of participants are better suited for a production scenario.
- The permissions are currently set in the constructor and can be modified through ``updatePermissionToView``. A more comprehensive system for managing different permissions levels, possibly including a way to revoke permissions is expedient.
- The system's reliance on correct address input is crucial. Adequate off-chain security measures will ensure that addresses correspond to the correct, authenticated participants.
- The contract lacks functions to remove permissions or to update the list of authorized nodes. In addition, emergency stop ("circuit breaker") patterns could be implemented for added security.

For real-world applications, especially concerning sensitive healthcare data, it is worth mentioning that rigorous security audits, testing, and contract code reviews will be performed before deployment.

b) Contract with dynamic addition and verification of participants

The breakdown of a dynamic and applicable smart contract model, with a focus on the ``AccessControl`` and ``DataContract`` is as follows:

These contracts aim to manage permissions for nodes in a blockchain network, specifically for viewing and storing healthcare data within a smart home healthcare ecosystem. The dynamic design ensures that data is ethically disclosed only to those entities that have the appropriate permissions, with enhanced security, flexibility, and data privacy provisions.

1). AccessControl Contract:

- State Variables:
 - ``owner``: Stores the Ethereum address of the owner — the account that deploys the contract.
 - ``authorisedNodes``: A mapping to keep track of which addresses (nodes) are authorized, this remains unused in the provided code and could be removed or implemented as needed.
 - ``permissions``: A private mapping from addresses to an integer representation of their specific permissions, which can be None (0), View (1), or Store (2).
- Events:
 - ``PermissionUpdated``: Triggered when the permission of a participant is updated (set or revoked).
- Modifiers:
 - ``onlyOwner``: Ensures that only the contract's owner can execute the function it's applied to.
 - ``authorisedToStore``: Ensures that the function can only be executed by an address with the 'Store' permission.
 - ``authorisedToView``: Ensures that the function can only be executed by an address with the 'View' permission.
- Constructor:
 - Sets the contract's deployer as the owner and assigns them the 'Store' permission by default.
- Functions:
 - ``setPermission``: Allows the owner to grant a specific permission (View or Store) to an address. It checks for valid input and triggers the ``PermissionUpdated`` event.
 - ``revokePermission``: Allows the owner to revoke any permissions assigned to an address, setting it to 'None', and triggers the ``PermissionUpdated`` event.
 - ``getPermission``: Returns the permission type of a specific address.

2). DataContract (inherits from AccessControl):

- State Variable:
 - ``dataHash``: A private string meant to hold an IPFS hash, representing the location of data stored off-chain. It is made private to ensure controlled access.
- Event:
 - ``HashUpdated``: Triggered when the IPFS hash (``dataHash``) is updated.
- Functions:
 - ``updateDataHash``: Allows an address with 'Store' permission to update ``dataHash``. It requires that the new hash is not empty and triggers the ``HashUpdated`` event.
 - ``getDataHash``: Returns the current ``dataHash`` value but only for addresses with 'View' permission.

An explanation of the workflow of the publisher-subscriber contracts is as follows:

- The contract owner deploys the ``AccessControl`` contract. By default, the owner has 'Store' permission.

- The owner can then set or revoke permissions for participants using ``setPermission`` and ``revokePermission``, providing flexible and dynamic access control. The changes in permissions are publicly logged through the ``PermissionUpdated`` event.
- Once participants have the appropriate permissions, they interact with the ``DataContract``:
 - o Participants with 'Store' permission can update the IPFS hash using ``updateDataHash``, which holds the off-chain data (potentially sensitive healthcare information). The update is logged through the ``HashUpdated`` event.
 - o Participants with 'View' permission can access the current data hash using ``getDataHash``, ensuring they only access data they are authorized to view.
- The system ensures data privacy by keeping ``dataHash`` private and making it accessible only through controlled functions.

Security Considerations:

- The updated contract enhances security by allowing dynamic permission management and enforcing strict access control to critical functions.
- It introduces input validation and error messages, providing clearer insights into any issues that participants encounter.
- The contract ensures data privacy by making the data hash a private variable.
- Despite these improvements, rigorous testing and a professional security audit are still paramount, especially when dealing with sensitive healthcare data.

This dynamic contract code version promotes a more secure, flexible, and privacy-focused approach to managing permissions and data access in the smart home healthcare ecosystem. However, continuous improvement and adherence to best practices are vital in maintaining robust security and functionality.

In comparing the two approaches for designing an applicable publisher-subscriber contract, the dynamic addition and verification of participants is better suited, and here are the key changes and improvements over the hardcoded version:

For encapsulation of access control:

- Introduction of a dedicated `AccessControl` contract to handle permission-related logic, improving the modularity and readability of the code.

For improved permission management:

- Added a `None` type to the `PermissionType` enum to represent the absence of permissions explicitly.
- Introduced a `setPermission` function to dynamically set permissions for an address.
- Added a `revokePermission` function to remove an address's permissions, enhancing the security and flexibility of permission management.
- Permissions are now directly mapped to an enum type, removing ambiguity and improving readability.

For data privacy:

- Made `dataHash` a private variable, ensuring it is only accessible through the `getDataHash` function, which includes appropriate access control checks.

For validation and error messages:

- Added requirements checks with descriptive error messages to ensure that functions are called with valid arguments.

For event enhancement:

- `PermissionUpdated` event now also emits the type of permission granted or revoked.

It is worth mentioning that smart contract codes require thorough testing, auditing, and potentially more features depending on the use case requirements, such as different levels of access control, sophisticated permission management, and emergency stop mechanisms. Moreover, the principle of least privilege could be considered i.e., grant only the permissions necessary for participants to perform their tasks.

More importantly, because this scenario involves medical data, compliance with healthcare regulations and data privacy standards like HIPAA or GDPR should be taken into consideration.

3.2.3 On the Strategies for Evaluating the Solution's Performance

To effectively evaluate the performance of the proposed authorisation framework, some evaluation metrics could be considered.

3.2.3.1 Performance Evaluation

The permission BC-based framework is proposed for providing and ensuring improved data security and privacy in the smart home setting through a lightweight hybrid encryption scheme as earlier described. In addition, though the PoA consensus algorithm does not perform mining, the BC-based architecture is likely to still incur slight computational and packet overhead on the nodes for the processes involved. To provide an appreciable evaluation at this stage, two different and logical traffic flow patterns classified as periodic and query-based could be implemented to evaluate these overheads [165, 236]. The evaluation metric of the packet, time, and energy overheads is applicable for performance evaluation. To assess the security resilience, scalability, and storage query efficiency, the overheads of the PoA-based BC architecture can be compared to those recorded from a baseline scenario that handles data transaction of SoPAD/ED without any tangle form of transport encryption, which includes using a traditional DBMS. However, the focus should not only be on low overheads but on other trade-offs to achieve significant security and privacy benefits.

3.2.3.2 Resilience Testing Procedure

This test is required to assess the resilience of the authorisation security framework. Threat models such as interception attacks often threaten the confidentiality and integrity of data, and by extension deprives smart homeowner of their data (SoPAD/ED) privacy. Therefore, to investigate the performance efficiency of the proposed authorisation framework towards ensuring privacy, the use of cryptanalysis is performed when testing the resilience of the proposed security framework in securing private data. On one hand, a Shellcode injection (i.e., via malware and botnet) can be launched into the system through a simulation that mimics an infected PDA that has been used on a public Wi-Fi infrastructure. The code injection attacks employed are to assess if the pattern of data collection and transport within the smart home healthcare ecosystem can be eavesdropped on before a brute force attack is used to intercept data, and if possible, modify the data before an off-chain or on-chain storage. Another attack scenario is to gain access to steal the private keys used for signing data in transit or gain access to search exposure/misplaced contract calls. Lastly, the smartwatch can be compromised through a corrupted version of the API developed for collecting the activity level data. A malicious prompt for an update of the app if executed, could infect the watch with a botnet. The home Wi-Fi is semi-trusted, but it can be assumed that an HTTPS protocol is configured as the transport service for sending data to the home gateway from the watch and indoor environment sensor, at least to alleviate further fear of interception within the home network, including insider attack. The code injection attacks can be used to simulate targeted interception attacks on the smart care home ecosystem to compromise devices, infiltrate networks, truncated services or applications (i.e., for interruption attack/DDOS), or

masquerade as an authorised entity. End-to-end encryption (E2EE) ensures that data is encrypted from the point of collection (e.g., the smartwatch) to its final destination (e.g., IPFS or the eHealth expert node). This encryption should persist while data is in transit through intermediate points like the home gateway. Testing the resilience of E2EE involves attempting to intercept the data at various points in its journey and verifying that it remains unintelligible due to encryption.

Cryptanalysis is the study of analyzing information systems to study the hidden aspects of the systems. It is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown. In other words, cryptanalysis is the art of deciphering encrypted data without access to the secret key used to initially encrypt the data. The experience in the cryptanalysis domain has revealed that evaluating the security level of a cryptosystem involves not only understanding the mathematical concept but also the application of the best possible cryptographic attacks on such cryptosystem to test its resilience by using the best available techniques [288]. Therefore, with the application of an appropriate attack on the resource-constrained platform, the security limits of the studied cryptographic algorithms can be determined, and this allows for recommendable adjustments to be made to the corresponding parameters of the proposed algorithm. In essence, cryptanalytical tasks in the scenario of study will be tailored towards constrained systems and those not high-end, requiring massive computations but rather nodes fitting the characteristics of the PoA consensus algorithm for privacy preservation in smart home settings. Furthermore, Public Key Infrastructure (PKI) and Key Management can be implemented to test a robust PKI to ensure that only the intended recipients can decrypt the data. This can include using digital certificates for authenticating the communicating parties. This test procedure can make the key exchange mechanism robust and resilient to attacks like Man-in-the-Middle (MiTM), where an attacker might try to impersonate one of the nodes. Table 16 illustrates some exploited vulnerabilities in DLT, including those related to theft/loss of private keys.

IPFS Security checks can be performed to make certain that any sensitive data is encrypted before being stored on IPFS. While IPFS provides content addressing and tamper-proofing, it does not natively encrypt data. It is equally important to test the access controls of the IPFS node and ensure that data cannot be accessed by unauthorized parties. A thorough audit and testing of the smart contracts code could also ascertain smart contract security. This should include known vulnerabilities like reentrancy attacks, overflow/underflow bugs, etc. Additionally, given the concern with data interception, safeguards should be in place to make sure contract logic does not inadvertently expose sensitive information, and only permitted addresses can execute certain functions. Wi-Fi security, network segmentation within the home, penetration testing, and blockchain node security are possible ways to perform resilience evaluation to toughened networks that parade private data.

Furthermore, input validation approaches such as whitelisting validation (inclusion or positive validation) and blacklist validation (exclusion or negative validation) are applicable. However, blacklist validation is favored since signature algorithms (binary patterns) not allowed to gain access to the smart home system are pre-defined. In this way, the proposed secure framework should be resilient enough to detect, attribute, and identify stages of interception attack life cycle, and deal with new or current versions of existing threats. Moreover, the elements within the publisher-subscriber-client smart contract algorithm contain the privacy-aware fine-grained access control mechanism expected to exclude smart home actors/ entities that do not follow protocol. A privacy model underpins this concept and will be presented during the privacy assessment criteria.

Table 16

Recent blockchain attacks and exploits

Top Five Blockchain Attacks	Loss and “in-actions”	Five DLT Vulnerabilities
<i>Wormhole</i> – February 2022 , Solana Platform	\$326M, fund returned in 24hrs	Exit scam
Bit Mart – 2021 , Ethereum Platform	\$150,000 asset, Hacked Private Key	51% Attack – majority attack, - Control of more than 50% of the hashing power on a blockchain.
<i>Poly Network</i> - August 2021	\$ 600m, misplaced “ contract call” intercepted. Hacked private key returned by some anonymous	Defi – Decentralised Finance - P2P system using smart contracts in decentralised blockchain networks.
MT Gox , 2011 – February, 2014	Up to \$4.7 billion, the greatest Bitcoin exchange robbery, MT Gox bankrupted	Exchange Hack - Social engineering hacks and persuasion tricks.
<i>Liquid Global</i> – August 2021 , Japanese Cryptocurrency Exchange	\$97M unauthorised user(s) access to wallet, > 78% of damage due to Ethereum-based asset	Phishing

3.2.3.3. Procedure for Privacy Assessment.

Given the complexity of the smart home healthcare ecosystem system and the paramount importance of privacy, particularly in the context of healthcare data, there is no single testing procedure that can act as a panacea. However, a comprehensive approach that combines various methodologies could provide a robust defense strategy. Among these, Privacy Impact Assessment (PIA) stands out as a particularly effective tool for identifying and mitigating privacy concerns in information systems, especially when used in combination with other methods like LINDDUN and STRIDE.

Privacy Impact Assessment (PIA) is a systematic assessment that identifies the impact a design might have on the privacy of individuals and sets forth recommendations for managing, minimizing, or eliminating that impact. While PIA itself is a broad framework, it can be particularly effective when tailored to the specific needs of your healthcare ecosystem. Methods that can be adopted to structure a PIA are as follows:

i). Description of the Information Flow: This clearly describes how information is collected, stored, used, and shared in the system. It includes data from the smartwatch, through the home gateway, within the blockchain, and in off-chain storage (IPFS). This also includes understanding who has access to what data, under what circumstances, and what controls are in place to prevent unauthorized access.

- ii). **Identification of Privacy Risks:** This identifies risks to individual privacy by considering how information is managed throughout its life cycle. This includes risks from unauthorized access, disclosure, alteration, and destruction. The LINDDUN framework is suitable here because it is designed to uncover privacy threats in software systems.
- iii). **Assessment of Privacy Risks:** This is applied to assess the potential impact of risks on the privacy of individuals. It considers both non-technical and technical aspects, including how data encryption, smart contract logic, or blockchain access controls might fail or be circumvented.
- iv). **Mitigation Strategies:** This involves developing strategies to mitigate each identified risk. The process could include technical measures, such as enhancing encryption or access controls, and non-technical measures e.g., establishing policies for how data should be handled or shared.
- v). **Documentation and Compliance:** This involves documenting the process and outcomes of the PIA, ensuring compliance with relevant health data protection regulations (e.g., GDPR, HIPAA). Such documentation can be vital for regulatory compliance and for communicating privacy practices to stakeholders.
- vi). **Regular Review:** Since privacy risks can evolve, the designed system can as well. Therefore, it is necessary to regularly review and update the PIA to handle new threats, vulnerabilities, or changes in the smart home healthcare system.

The use of a PIA in conjunction with threat modeling tools like LINDDUN and STRIDE can provide a comprehensive view of privacy risks. While LINDDUN is focused on privacy, STRIDE provides a broader view of security threats. Using both can assist in ensuring a wide range of potential issues are being considered.

In implementing these methodologies, collaboration with stakeholders, including cybersecurity experts, legal advisors, healthcare professionals, and patient advocates, can enhance the effectiveness of privacy protection measures and adoption. The goal is not just to protect data from interception or unauthorized access, but also to maintain trust among users and stakeholders by ensuring that the system respects and upholds individuals' privacy rights.

A combination of LINDDUN and STRIDE is suggested as a means of evaluating the threat model of the secure authorisation framework designed for our scenario. Fig. 30 depicts the threat analysis of both models with the LINDDUN framework more focused on the provision of extensive procedural and knowledge support to systematically tackle privacy threat elements and for the elicitation and mitigation of privacy threats in software application systems. LINDDUN's methodology consists of 3 main steps: (1) Model the system, (2) Elicit threats, and (3) Manage threats. The six steps of this privacy assessment tool are categorised into problem and solution spaces.

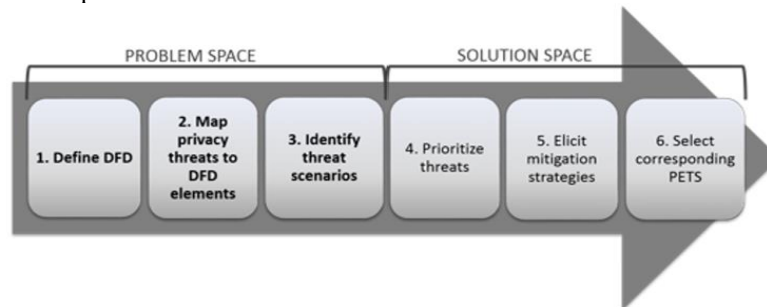


Fig. 30. Overview of LINDDUN [189]

LINDDUN is mnemonic for **L**inkability, **I**dentifiability, **N**onrepudiation, **D**etectability, **D**isclosure of Information, **U**nawareness and **N**oncompliance. These six steps provide a systematic approach to privacy assessment, but disclosure of information is the primary focus considered to handle privacy concerns as well as data security examined in the course of this study. Moreover, as a suitable and alternative privacy assessment criterion, identity spoofing, data tampering, information disclosure and elevation of privilege are specific threats violating authentication, integrity, confidentiality, and authorisation among others when examined using STRIDE for threat evaluation. **Table 17** further illustrates the applicability of STRIDE.

Table 17

Illustration of STRIDE application to privacy assessment

Mnemonic	Threat	Security Violated	Threat Description
S	Spoofing	Authentication	Identity pretense, masquerading e.g., Sybil attack.
T	Tampering	Integrity	Data, software or network modification, fabrication.
R	Repudiation	Non-repudiation	Denial of actions, honest but curious behaviours.
I	Information Disclosure	Confidentiality	Unauthorized information access.
D	Denial of Services	Availability	Exhausting resources required for services provision or theft of resources.
E	Elevation of Privilege	Authorisation	Granting unauthorized access.

3.4. Decision-making Scheme to Enhance a Privacy-preserving Smart Home Healthcare System

A dynamic model of privacy that provides a pattern of computing data transaction process as expected by nodes designated for acquisition (collection), storage, and monitoring using underlying PoA-based blockchain is considered in decision-making for ethical disclosure of private data in our smart home healthcare scenario. This solution assessment is based on the analysis of various data security and privacy issues encountered when transporting sensitive data in IoT-based smart home systems. To this effect, the anticipated authorisation framework for the ethical disclosure of private data approaches the deprivation of user privacy from the perspective of data leakage or lack of data confidentiality.

To proffer solutions to privacy issues, all phases of the data value chain are considered, including acquisition/collection, storage, and use. Proponents of privacy preservation in [135, 290] suggested two practicable solutions e.g., privacy by design, and privacy enhancing technologies (PET). However, an approach that adopts the concept of privacy by design/default is a better fit for the smart home healthcare system. Authors in [291] studied and proposed a similar implementation that integrated privacy protection into both technologies such as computer chips, networking platforms, and organizational policies i.e., in privacy impact assessments. Therefore, a precise privacy model is considered to preserve data privacy while maintaining the utility of the system. In a similar manner, [23] utilised differential privacy to ensure the confidentiality of viewable data in a privacy-preserving framework for access control and interoperability of electronic health records, but the differential privacy scheme added noise to the blockchain's transactions, thereby, limiting the transaction scalability of the blockchain from storing data on-chain. Hence, a decision-making model for privacy preservation is proposed as an integral component of the underlying smart contract-enabled blockchain implementation.

3.4.1. Process Model for Data Classification in Smart Home Healthcare System

In discussing a model for ensuring the security of private data within a smart home healthcare system. The system's process hinges on two primary components: Permissibility and Authorisation-level, which are determined by the data owner. This security model is inherently stochastic, meaning it is probabilistic and considers the randomness and unpredictability of certain variables. The process is broken down as follows:

a). Independent Variables (X): These are factors classified as 'Permissibility,' which are further divided into two categories:

- i). Set of Personal Activity Data (SoPAD): This could include any data related to the personal activities of the elderly individual residing in the smart home, such as their activity level data (most especially those that a smartwatch can collect e.g., accelerometer and gyroscope data), daily routines, health data, personal preferences, etc.
- ii). Environmental Data (Ambient Data): This encompasses data related to the environment of the smart home, possibly including temperature, pressure, humidity, lighting, air quality (AQ), gas, sound levels, etc.

These independent variables influence the level of access granted to different entities trying to interact with the data owner's private information.

b). Dependent Variable (Y) - Authorisation-level: This represents the level of access granted and is influenced by the independent variables. It is categorized into three levels:

- Access
- Store
- Monitor

This dependent variable is binary, meaning each level can either be allowed (1) or denied (0), representing the data owner's decision to permit or refuse the respective actions on their private data.

The relationship between the independent and dependent variables is examined using a Multinomial Logistic Regression model. This model is particularly suitable because the dependent variable is categorical with more than two categories, and the outcome is binary. The model estimates the probabilities of the different possible outcomes of a categorically distributed dependent variable, given a set of independent variables.

In summary, one can say logit regression references the binomial distribution and estimates the probability (π) of an event occurring ($Y=1$) rather than not occurring ($Y=0$) from a knowledge of relevant independent variables e.g., ($k_1[\text{Accelerometer_data}]$, $k_2[\text{Gyro_data}]$, and $k_3[\text{AQ_data}]$). Maximum Likelihood (MLE) is an iterative process used to estimate regression coefficients. Therefore,

π is for Probability that $Y = 1$, and

$1 - \pi$ for Probability that $Y = 0$

then the logistic model is:

The logistic model described is as follows:

$$\Omega = f(X) = \log\left(\frac{\pi}{1-\pi}\right) = \beta_0 + \beta_1 X \quad (1)$$

Where:

- Ω is the log-odds (the logarithm of the odd $\pi/(1-\pi)$),
- π is the probability of the event occurring ($Y=1$),
- X represents the independent variables,
- β_0 and β_1 are the coefficients to be estimated in the model

Thus, if the antilog (exponential operator) e is applied to both sides of equation (1), we get the value of the odd:

$$O = e^{\log\left(\frac{\pi}{1-\pi}\right)} = e^{\beta_0 + \beta_1 X} \quad (2)$$

Taking the antilog gives the odds ratio, not the probability, but it is related to the probability and changes in a predictable way with X , the independent variable.

The final logistic model expression used for prediction is:

$$Y = \frac{e^{\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n}}{1 + e^{\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n}} \quad (3)$$

where Y is the predicted probability that the event of interest occurs.

The decision-making regarding privacy preservation is then based on modeling the expected security of private data, considering the behavior of each node in the network. The expectation is binary: either deny (0) or allow (1) access. The "privacy" for each node in a blockchain network (BCN) is evaluated using a sigmoid function, which considers the number of allow and deny actions a node performs. This is encapsulated in the equation:

$$Privacy_n^{(i)} = \frac{1}{1 + e^{-\alpha(\#allow - \#deny)}} \quad (4)$$

In this equation 4:

- $Privacy_n^{(i)}$ represents the privacy model for every node,
- α is a parameter of the model (potentially relating to the sensitivity of the response to changes in the difference between allow and deny actions),
- $\#allow - \#deny$ represents the net trustworthiness measure of a node, based on its previous actions.

This model thus provides a dynamic and probabilistic assessment of each node's privacy level in the network, which can be used to make informed decisions about data security and access permissions in the smart home healthcare system.

The decision is to know how we can effectively model the relationship between permissibility and authorisation-level variables by modeling the expected security on private data that is suggested from the behavior of each node in the future as authorisation policies are put in place. The behaviour of authorisation-level in the future has only binary outcomes to either deny (0) or allow (1) access. The expected value of privacy of personal data is a probability P since it involves a binary random variable. This probability is approximated by considering the number of allow and deny actions a trustworthy node performs and then utilize a sigmoid function to squash it into a probability. Thus, for every block i which decides the node weight to select the allow or deny transaction, the privacy model for every node of the permissioned BCN is re-evaluated. Hence, the following:

- A new dynamic measure of privacy is proposed which represents the expected value of privacy in each node (n) for every block (i) that predicts the probability of a node behaving well in the future. This is simply the estimate of the probability P where allowable transactions that follow protocol are rewarded with access rights and is explained by the sigmoid function.
- The sigmoid function plays an important role in the context of logistic regression, where logistic regression is a technique to predict the outcome of binary classification problems.
- In this study, the *multinomial logistic regression model* explains the relationship between functional input X as factors of permissibility as an independent variable; and single dependent variable Y for authority level which has 3 levels namely *acquire (access)*, *store*, and *monitor* transactions of the data subject, and each level has a binary outcome, i.e., to either allow (1) or deny (0) the transaction.
- The sigmoid function plays the role of an activation function by taking the weighted sum of the functional input factors and outputs the probability value. For any value of x, the sigmoid function will output a value between 0 and 1.
- The limits of the power of the exponential in the multinomial logistic regression model are expressed in equation 3; and using the sigmoid function, equation 3 can be squashed into equation 4.
- For the sigmoid function, the profile of the limits of the sigmoid function is utilised to re-evaluate the privacy model of every node as seen in equation 4:

With this procedure, the BCN attaches more importance (e.g., gives more weight) to trusted nodes that decide and validate transactions by either allowing or denying them. [Table 18](#) is a summary of the proposed privacy model description.

Table 18

Summary of the system process model for data classification to demonstrate the planned privacy preservation process in the presented scenario.

<i>Model</i>	<i>Actions</i>
Functional <i>input</i> data (X) are <i>factors of permissibility</i> : (Y) represents <i>authorisation-level</i> :	identified as <i>independent variables</i> categorised into SOPAD and AD identified as <i>a single dependent variable</i> , categorized into three levels, namely <i>store</i> , <i>access</i> , and <i>monitor</i> transactions of data subjects. - Each level has a binary outcome, i.e., to either allow (1) or deny (0) the transaction.
<i>Regression Analysis</i> :	used to describe the nature of the relationship between (X) and (Y) above
<i>Logistic (logit) Regression</i> :	to test if changes in the predictor variables (X) of permissibility are associated with changes in the response variable (Y) of authorisation-level .
<i>Regression coefficients estimated using Maximum Likelihood Estimation</i> (i.e., iterative process):	- estimates the probability (π) of an event occurring (Y=1) rather than probability ($1 - \pi$) of not occurring (Y=0), having knowledge of relevant independent variables (k_1, k_2 and k_3).
<i>The logistic model is:</i>	$\Omega = f(X) = Y = \log\left(\frac{\pi}{1-\pi}\right) = \beta_0 + \beta_1 X \quad (1)$
<i>the value of the odd:</i> antilog (exponential operator) e applied to both sides of eqn (1) Where β_0 is now the value of the odd when $X = 0$	$O = e^{\log\left(\frac{\pi}{1-\pi}\right)} = e^{\beta_0 + \beta_1 X} \quad (2)$
<i>Multinomial logistic regression model (log of odd ratio)</i> is the specific regression analysis for understanding variation in the probabilities for examining the <i>system process of permissibility and access-right</i> and expressed as:	$Y = \frac{e^{\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n}}{1 - e^{\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n}} \quad (3)$
<i>Sigmoid function</i> : - to make <i>predictions</i> for data security and <i>decision</i> -making in BC. - by <i>counting the number of allow and deny actions a trustworthy node, n</i> , performs; the <i>sigmoid function</i> is used to <i>squash(summarizes)</i> it into a probability. i.e., $Privacy \propto Resources(n)$	we re-evaluate the privacy model of every node as: $Privacy_n^{(i)} = \frac{1}{1 + e^{-\alpha(\#allow - \#deny)}} \quad (4)$
	Where α is the step size

4. Conclusion

The article performed a critical review of unresolved issues and open challenges faced on data security and user privacy in IoT-based applications such as in the smart home healthcare system, a combination of both smart home and smart healthcare. Smart healthcare is a potential use case where the security requirement analysis and authorisation framework have been proposed to provide the requisite solution. The examined technique considered the adoption of blockchain

technology as an underlying service to improve data integrity, and to deploy a privacy model borne out of consent (e-consent) and acceptance of the data owner to enhance data distribution and transaction validation performed within the PoA consensus algorithm process that validates transactions and creates blocks; an efficient lightweight hybrid encryption scheme fit for resource constrained environment to provide data confidentiality and by extension users privacy; provide efficient, decentralised and secure data storage and fine-grained access control through smart contracts to ensure ethical disclosure of private data in smart home health ecosystem. Moreover, the paper also reviewed opportunities and solutions that focused on the integration of IoT and blockchain (BCoT) with other technologies to prevent data interception and leakage and ensure privacy preservation in several domains with similar data security concerns to that of smart healthcare. In several use cases, the adoption of blockchain was useful, efficient, and suitable. However, it is necessary to continue to test out if the healthcare domain requires the integration of blockchain or not, due to the volatility of relevant health data protection regulations (e.g., HIPAA, GDPR), which at times requires a whole new thinking. Moreover, privacy concerns in healthcare require stringent ethical analysis, approval, and documentation since privacy risks can evolve, thereby provoking new regulatory compliance for communicating privacy practices to stakeholders.

Specific problems addressed in the research questions investigated in this article revealed the need for an authorisation framework that implements a permissioned PoA-based blockchain as a building block and a privacy model for decision-making within the blockchain network to support ethical disclosure of private data in the healthcare realm. Publisher-subscriber smart contract algorithm is also introduced to ensure access control from the context of patient empowerment and information stakeholder engagement. Moreover, several approaches toward implementation can be done using different features of blockchain to achieve the aims desired in RQ 1-5. The suggested approach leverages publisher-subscriber contracts for access control. In addition, the classification of permission authority, specific layers of smart contracts, control authority, ethics, and governance rules across multiple healthcare services is explorable and extensible for future work. Ongoing research work aims to provide more findings from test-bed implementation.

In conclusion and further critiquing blockchain DLT, one of the most frequently asked questions when presenting blockchain technology is "When will this technology be widely used?". In some ways, the technology is already well-established. Blockchain-based cryptocurrencies are an undeniable force within the payment world, with a market value of several billion dollars and multiple well-funded exchanges. They have been a success even if they may eventually be replaced. Most firms and sectors can continue to thrive even if they do not implement blockchain into their operations. Aside from that, this review highlights cases that are not limited to payment services or digital currencies. People are concerned about blockchain 2.0 implementations and how they will affect their sector, as well as the possibility that competitors will incorporate these technologies more quickly, putting them at a disadvantage. On the other hand, organisations do not want to invest in a volatile trend, so the fact that prestigious firms are investing heavily in these technologies is a testimony to their relevance. The most pressing question is not if but *when* blockchain resources will progress from being cutting-edge technology to enterprise-ready solutions. It is too soon to speculate; however, it is worth considering that blockchain solutions will have many applications. Every business is unique and requires different tools, and it is almost guaranteed that no "one-size-fits-all" blockchain system will ever exist.

Investment in blockchain technology, albeit coming mainly from private sources, is expected to increase and be extended by governmental initiatives. Blockchain has brought together many of the brightest and most enterprising individuals across different sectors, transforming into a shining hub of enterprising and technological advances. It connects three of the greatest fields of our time: technology, currency, and democracy. Its power for transformation means that individuals like ourselves can achieve more control over our information, data, and, ultimately, our lives. This is what democracy is supposed to look like in the Information Age. In a world where internet companies are monopolizing our online identities, blockchain may be able to empower users to take back this perceived lack of control. However, we should be prepared for the insecurities that it might bring with it.

Compliance with Ethical Standards

CRediT authorship contribution statement

Olusogo Popoola: Writing – original draft, Writing – review & editing. **Marcos A. Rodrigues:** Review & editing. **Jim N. Marchang:** Review & editing. **Alex Shenfield:** Review & editing. **Augustine Ikpehia:** Review & editing. **Jumoke Popoola:** Review & editing.

Acknowledgments

I would like to thank my supervisory team for the inspiration and assistance offered during the development and revision of this article.

Disclosure of potential conflicts of interest

The authors declare that this manuscript has no conflict of interest with any other published source and has not been published previously (partly or in full). No data have been fabricated or manipulated to support our conclusions.

Author Contributions

All authors have equally contributed to this work and read and agreed to the published version of the manuscript.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of Competing Interest

The authors of this research article declare that no conflict of interest in preparing this research article.

Data availability

No data was used for the research described in the article.

References

- [1] R. Neisse, G. Steri and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking.," *In Proceedings of the 12th international conference on availability, reliability and security*, 2017.
- [2] W. Wang, X. Li, X. Qiu, X. Zhang, J. Zhao and V. Brusic, "A privacy-preserving framework for federated learning in smart healthcare systems.," *Information Processing & Management.*, vol. 60, no. 1, p. 103167, 2023.
- [3] T. K. Landauer, "Research methods in human-computer interaction.," *In Handbook of human-computer interaction. North-Holland*, pp. 905-928, 1988.
- [4] J. Lazar, J. H. Feng and H. Hochheiser, Research methods in human-computer interaction., Morgan Kaufmann., 2017.
- [5] L. K. Ramasamy, F. Khan, M. Shah, B. V. V. S. Prasad, C. Iwendi and C. Biamba, "Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring.," *Sensors.*, vol. 22, no. 3, p. 1076, 2022.
- [6] A. S. Rajasekaran, A. Maria, M. Rajagopal and J. Lorincz, "Blockchain Enabled Anonymous Privacy-Preserving Authentication Scheme for Internet of Health Things.," *Sensors.*, vol. 23, no. 1, p. 240, 2023.
- [7] W. Li, T. Yigitcanlar, A. Liu and I. Erol, "Mapping two decades of smart home research: A systematic scientometric analysis," *Technological Forecasting and Social Change.*, vol. 179, p. 121676., 2022.
- [8] J. Bugeja, A. Jacobsson and P. Davidsson, "On privacy and security challenges in smart connected homes.," *In 2016 European Intelligence and Security Informatics Conference (EISIC). IEEE.*, pp. 172 -175, 2016.
- [9] W. Ali, G. Dustgeer, M. Awais and M. A. Shah, "IoT based smart home: Security challenges, security requirements and solutions.," *In 2017 23rd International Conference on Automation and Computing (ICAC). IEEE.*, pp. 1-6, 2017.
- [10] I. Butun, A. Sari and P. Österberg, "Security implications of fog computing on the internet of things," *In 2019 IEEE International Conference on Consumer Electronics (ICCE) IEEE.*, pp. 1 - 6, 2019.
- [11] O. Cheikhrouhou, O. B. Fredj, N. Atitallah and S. Hellal, "Intrusion Detection in Industrial IoT.," *In 2022 15th International Conference on Security of Information and Networks (SIN) IEEE.*, pp. 01-04, 2022.
- [12] E. M. Schomakers, H. Biermann and M. Ziefle, "Users' preferences for smart home automation—investigating aspects of privacy and trust.," *Telematics and Informatics.*, vol. 64, p. 101689, 2021.
- [13] J. K. Burgoon, "Privacy and communication.," *Annals of the International Communication Association.*, vol. 6, no. 1, pp. 206 - 249, 1982.
- [14] H. Nissenbaum and T. Wong, "Review Essay—Helen Nissenbaum's Privacy in Context: Technology, Policy, and the Integrity of Social Life," *German Law Journal.*, vol. 12, no. 3, pp. 957-967, 2010.
- [15] I. Altman, "Privacy - A conceptual analysis.," *Environment and behavior.*, vol. 8, no. 1, pp. 7 -29, 1976.
- [16] S. Lahlou, "Identity, social status, privacy and face-keeping in digital society.," *Social science information.*, vol. 47, no. 3, pp. 299-330, 2008.
- [17] P. Pirzada, A. Wilde, G. H. Doherty and D. Harris-Birtill, "Ethics and acceptance of smart homes for older adults," *Informatics for Health and Social Care*, vol. 47, no. 1, pp. 10 - 37, 2022.
- [18] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra and C. Colautti, "Privacy calculus model in e-commerce—a study of Italy and the United States.," *European Journal of Information Systems.*, vol. 15, no. 4, pp. 389-402, 2006.
- [19] F. Kehr, T. Kowatsch, D. Wentzel and E. Fleisch, "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus.," *Information Systems Journal.*, vol. 25, no. 6, pp. 607 -635, 2015.
- [20] S. Furnell, R. Esmael, W. Yang and N. Li, "Enhancing security behaviour by supporting the user," *Computers & Security.*, vol. 75, pp. 1 - 9, 2018.
- [21] Himanshi, "Consensus Mechanisms in Blockchain," 27 January 2023. [Online]. Available: <https://www.shiksha.com/online-courses/articles/consensus-mechanisms-in-blockchain>. [Accessed 30 January 2023].
- [22] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data.," *In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE.*, pp. 51 -55, 2018.
- [23] G. G. Dagher, J. Mohler, M. Milojkovic and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology.," *Sustainable cities and society*, vol. 39, pp. 283-297, 2018.
- [24] R. Zhang, R. Xue and L. Liu, "Security and privacy on blockchain.," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, pp. 1 -34, 2019.

- [25] A. Jøsang, "A consistent definition of authorization. In Security and Trust Management," in *13th International Workshop, September 14–15, 2017, Proceedings 13* (pp. 134-144). Springer International Publishing., Oslo, Norway, 2017.
- [26] M. Kucharczyk, "What is a private blockchain and why do you need it?," 14 June 2021. [Online]. Available: <https://softwaremill.com/what-is-private-blockchain-why-do-you-need-it/>. [Accessed 10 September 2023].
- [27] V. Buterin, "On Public and Private Blockchains," 7 August 2015. [Online]. Available: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains>. [Accessed 1 December 2020].
- [28] A. Badshah, M. Waqas, F. Muhammad, G. Abbas and Z. H. Abbas, "A Novel Framework for Smart Systems Using Blockchain-Enabled Internet of Things," *IT Professional*, vol. 24, no. 3, pp. 73-80, 2022.
- [29] C. V. S. Aishwarya, J. Caleb Joel Raj, S. K. Mandal, C. N. Reddy and B. Mishra, "Smart Health Care by Harnessing the Internet of Things (IoT): Applications, Challenges, and Future Aspects.," *In IoT Based Smart Applications* (pp. 35-54). Cham: Sprin, pp. 35 - 54, 2022.
- [30] R. Krishnamurthy, "Bitcoin mining unsustainable; climate damages comparable to beef, natural gas, crude oil: Study," 03 October 2022. [Online]. Available: [https://www.downtoearth.org.in/news/renewable-energy/bitcoin-mining-unsustainable-climate-damages-comparable-to-beef-natural-gas-crude-oil-study-85266#:~:text=Roughly%2070%20kilowatt%20hour%20\(kWh,and%20natural%20gas%2C%20said%20Jones..](https://www.downtoearth.org.in/news/renewable-energy/bitcoin-mining-unsustainable-climate-damages-comparable-to-beef-natural-gas-crude-oil-study-85266#:~:text=Roughly%2070%20kilowatt%20hour%20(kWh,and%20natural%20gas%2C%20said%20Jones..) [Accessed 10 October 2022].
- [31] ITU-T, "Technical Report FG DLT D1.2 Distributed ledger technology overview, concepts, ecosystem," 1 August 2019. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf>. [Accessed 1 March 2021].
- [32] M. Xie, J. Liu, S. Chen and M. Lin, "A survey on blockchain consensus mechanism: research overview, current advances and future directions.," *International Journal of Intelligent Computing and Cybernetics, (ahead-of-print)*, 2022.
- [33] D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain technology overview.," *arXiv preprint arXiv*, p. 1906.11078., 2019.
- [34] X. Xu, G. Sun, L. Luo, H. Cao, H. Yu and A. V. Vasilakos, "Latency performance modeling and analysis for hyperledger fabric blockchain network," *Information Processing & Management*, vol. 58, no. 1, p. 102436., 2021.
- [35] T. Wall, "The Risk of "Credential Stuffing" to the Smart Home.," 28 March 2019. [Online]. Available: <https://www.iotforall.com/credential-stuffing>. [Accessed 19 June 2021].
- [36] B. A. A. I. Ali, "Cyber and physical security vulnerability assessment for IoT-based smart homes.," *Sensors*, vol. 18, no. 3, p. 817, 2018.
- [37] L. Ziani, M. E. Khanouche and A. Belaid, "Internet of Behaviors: A literature review of an emerging technology.," *In 2022 First International Conference on Big Data, IoT, Web Intelligence and Applications (BIWA) IEEE*, pp. 42-47, 2022.
- [38] D. Zafar, "The blockchain & data privacy (GDPR)," 11 November 2022. [Online]. Available: <https://cybersecurity.att.com/blogs/security-essentials/the-blockchain-data-privacy-gdpr>. [Accessed 13 February 2023].
- [39] Gartner, "Leading in a digital world: The dawn of the digital industrial economy.," in *Gartner Symposium/ITxpo 2013, 28 – 31 October*, Gold Coast, Australia , 2013.
- [40] R. Meulen, "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015," 11 November 2014. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2014-11-11-gartner-says-nearly-5-billion-connected-things-will-be-in-use-in-2015>. [Accessed 15 March 2021].
- [41] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya and B. Balusamy, "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Computing and Applications*, vol. 32, pp. 639-647, 2020.
- [42] S. Cannizzaro and R. Procter, "How Is the Internet of Things Industry Responding to the Cybersecurity Challenges of the Smart Home?," *In Ubiquitous and Pervasive Computing-New Trends and Opportunities. IntechOpen*, 2022.
- [43] O. d'Angelis, L. Di Biase, L. Vollero and M. Merone, "IoT architecture for continuous long term monitoring: Parkinson's Disease case study.," *Internet of Things*, vol. 20, p. 100614., 2022.
- [44] J. Zhao, S. Zhang, Y. Sun, N. Zhou, H. Yu, H. Zhang and D. Jia, "Wearable optical sensing in the medical internet of things (MIoT) for pervasive medicine: Opportunities and challenges.," *Acs Photonics*, vol. 9, no. 8, pp. 2579-2599, 2022.
- [45] Y. Padarth and R. R. P. Kuppusamy, "IoT-Based Embedded Sensor System for Real-Time Health Monitoring of Composite Structures for Large-Scale Industrial Operations.," *In Industrial Automation and Robotics. CRC Press*, pp. 3-32, 2023.
- [46] C. V. S. Aishwarya, J. Caleb Joel Raj, S. K. Mandal, C. N. Reddy and B. Mishra, "Smart Health Care by Harnessing the Internet of Things (IoT): Applications, Challenges, and Future Aspects.," *In IoT Based Smart Applications. Cham: Sprin*, pp. 35 -54, 2022.
- [47] A. J. Perez, F. Siddiqui, S. Zeadally and D. Lane, "A Review of IoT Systems to Enable Independence for the Elderly and Disabled Individuals.," *Internet of Things*, p. 100653., 2022.
- [48] S. A. Ali and R. Khan, "IoT-based Technologies for Addressing the Unique Healthcare Needs of the Elderly Population.," *Preprints.org 2023, 2023030088*. <https://doi.org/10.20944/preprints202303.0088.v1.>, 2023.

- [49] A. Daniels, "The rise of private permissionless blockchains — part 1," 18 October 2018. [Online]. Available: <https://medium.com/tonetwork/the-rise-of-private-permissionless-blockchains-part-1-4c39bea2e2be>. [Accessed 10 September 2023].
- [50] M. Hamza and M. A. Akbar, "Smart Healthcare System Implementation Challenges: A stakeholder perspective.," *arXiv preprint arXiv:2208*, p. 12641, 2022.
- [51] X. Du, B. Chen, M. Ma and Y. Zhang, "Research on the application of blockchain in smart healthcare: constructing a hierarchical framework.," *Journal of Healthcare Engineering*, 2021., 2021.
- [52] A. I. Florea, I. Anghel and T. Cioara, "A Review of Blockchain Technology Applications in Ambient Assisted Living.," *Future Internet*, vol. 14, no. 5, p. 150, 2022.
- [53] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction.," *Journal of medical systems*, vol. 43, pp. 1-35, 2019.
- [54] W. Viriyasitavat, L. Da Xu, Z. Bi and D. Hoonsoopon, "Blockchain technology for applications in internet of things—mapping from system design perspective.," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8155-8168., 2019.
- [55] K. Gaikwad, K. Kulkarni, S. Kohle and P. Patil, "Implementation of Blockchain Technology in IOT Based Smart Home.," *In 2022 5th International Conference on Advances in Science and Technology (ICAST)*. IEEE., pp. 6 -10, 2022.
- [56] Z. K. Taha, C. T. Yaw, S. P. Koh, S. K. Tiong, K. Kadigama, F. Benedict, J. D. Tan and Y. A. Balasubramaniam, "A Survey of Federated Learning from Data Perspective in the Healthcare Domain: Challenges, Methods, and Future Directions. IEEE Access.," *IEEE Access*, 2023.
- [57] T. K. Mackey, T. T. Kuo, B. Gummadi, K. A. Clauson, G. Church, D. Grishin, K. Obbad, R. Barkovich and M. Palombini, "'Fit-for-purpose?'—challenges and opportunities for applications of blockchain technology in the future of healthcare.," *BMC medicine*, vol. 17, no. 1, pp. 1-17, 2019.
- [58] K. A. Clauson, E. A. Breeden, C. Davidson and T. K. Mackey, "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare:: An exploration of challenges and opportunities in the health supply chain.," *Blockchain in healthcare today*. <https://doi.org/10.30953/bhty.v1.20>, vol. 1, no. <https://www.blockchainhealthcaredtoday.com/index.php/journal/article/view/20>, 2018.
- [59] S. A. Bennacer, K. Sabiri, A. Aaroud, K. Akodadi and B. Cherradi, "A comprehensive survey on blockchain-based healthcare industry: applications and challenges," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 3, pp. 1558-1571., 2023.
- [60] R. Pathak, B. Soni and N. B. Muppalaneni, "Role of Blockchain in Health Care: A Comprehensive Study.," in *In Proceedings of 3rd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications: ICMISC 2022 (pp. 137-154)*, Springer Nature Singapore., 2022.
- [61] A. Pattanayaka and S. Dhala, "Blockchain in Healthcare.," *Preprint, Elsevier*, 2021.
- [62] M. S. Mahmood and N. B. Al Dabagh, "Blockchain technology and internet of things: review, challenge and security concern.," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 1, p. 718, 2023.
- [63] N. Kuriakose and D. Midhunchakkaravarthy, ". A Review on IoT Blockchain Technology.," *Indian Journal of Data Communication and Networking (IJDCN)*. DOI: [10.54105/ijdcn.F3719.123122](https://doi.org/10.54105/ijdcn.F3719.123122), vol. 3, no. 1, pp. 2582-760X, 2022.
- [64] D. Marbough, M. C. E. Simsekler, K. Salah, R. Jayaraman and S. Ellahham, "Blockchain for Patient Safety: Use Cases, Opportunities and Open Challenges.," *Data*, vol. 7, no. 12, p. 182, 2022.
- [65] Z. Wenhua, F. Qamar, T. A. N. Abdali, R. Hassan, S. T. A. Jafri and Q. N. Nguyen, "Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends.," *Electronics*, vol. 12, no. 3, p. 546., 2023.
- [66] B. S. Egala, A. K. Pradhan, P. Dey, V. Badarla and S. P. Mohanty, "Fortified-Chain 2.0: Intelligent Blockchain for Decentralized Smart Healthcare System.," *IEEE Internet of Things Journal*, 2023.
- [67] S. G. Alonso, J. Arambarri, M. López-Coronado and I. de la Torre Díez, "Proposing new blockchain challenges in ehealth.," *Journal of medical systems*, vol. 43, pp. 1 - 7, 2019.
- [68] A. Odeh, I. Keshta and Q. A. Al-Haija, "Analysis of Blockchain in the Healthcare Sector: Application and Issues.," *Symmetry*, p. 1760, 2022.
- [69] K. M. Abiodun, E. A. Adeniyi, J. B. Awotunde, C. Chakraborty, D. R. Aremu, A. A. Adebisi and M. O. Adebisi, "Blockchain and Internet of Things in Healthcare Systems: Prospects, Issues, and Challenges.," *In Digital Health Transformation with Blockchain and Artificial Intelligence*. CRC Press., pp. 1-22, 2022.
- [70] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård and R. Vitenberg, "A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions.," *IEEE Communications Surveys & Tutorials*, 2022.
- [71] R. Kumar, D. Singh, K. Srinivasan and Y. C. Hu, "AI-Powered Blockchain Technology for Public Health: A Contemporary Review, Open Challenges, and Future Research Directions.," *In Healthcare*. MDPI, vol. 11, no. 1, p. 81, 2022.
- [72] K. Pal, "A Decentralized Privacy Preserving Healthcare Blockchain for IoT, Challenges, and Solutions.," *In Prospects of Blockchain Technology for Accelerating Scientific Advancement in Healthcare*. IGI Global., pp. 158-188, 2022.

- [73] A. D. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT.," *Sensors.*, vol. 19, no. 2, p. 326, 2019.
- [74] Z. Ilyas, M. I. Tariq, S. K. Shahzad and R. A. Karim, "Resolving Smart Health Security Issues Using Ontologies and Blockchain Services," *Pakistan Journal of Emerging Science And Technologies (PJEST)*, vol. 3, no. 2, 2022.
- [75] R. Myrzashova, S. H. Alsamhi, A. V. Shvetsov, A. Hawbani and X. Wei, "Blockchain Meets Federated Learning in Healthcare: A Systematic Review with Challenges and Opportunities.," *IEEE Internet of Things Journal.*, 2023.
- [76] C. Choudhary, I. Singh and M. Shafiq, "Blockchain for IoT Security and Privacy: Challenges, Application Areas and Implementation Issues.," *Cross-Industry Blockchain Technology: Opportunities and Challenges in Industry 4.0, 1.*, 2022.
- [77] H. D. Zubaydi, P. Varga and S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review.," *Sensors.*, vol. 232, p. 788, 2023.
- [78] M. Attaran, "Blockchain technology in healthcare: Challenges and opportunities.," *International Journal of Healthcare Management.*, vol. 15, no. 1, pp. 70-83, 2022.
- [79] J. Andrew, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions.," *Journal of Network and Computer Applications.*, p. 103633., 2023.
- [80] Y. I. Alzoubi, A. Al-Ahmad, H. Kahtan and A. Jaradat, "Internet of Things and Blockchain Integration: Security, Privacy, Technical, and Design Challenges.," *Future Internet.*, vol. 14, no. 7, p. 216, 2022.
- [81] N. Adhikari and M. Ramkumar, "IoT and Blockchain Integration: Applications, Opportunities, and Challenges.," *Network. MDPI*, vol. 3, no. 1, pp. 115-141, 2023.
- [82] A. S. Makinde, S. Omaji, A. O. Agbeyangi and M. S. Alade, "Impact of Blockchain on the Security and Privacy of IoT-Empowered Healthcare Systems.," *In Contemporary Applications of Data Fusion for Advanced Healthcare Informatics. IGI Global*, pp. 319-349, 2023.
- [83] A. S. Makinde, A. O. Agbeyangi and S. Omaji, "Integration of Blockchain Into Medical Data Security: Key Features, Use Cases, Technical Challenges, and Future Directions.," *In Contemporary Applications of Data Fusion for Advanced Healthcare Informatics. IGI Global.*, pp. 137 -165, 2023.
- [84] S. Gupta, H. K. Sharma and M. Kapoor, "Application and Challenges of Blockchain in IoMT in Smart Healthcare System.," *In Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Cham: Springer International Publishing.*, pp. 39-53, 2022.
- [85] M. Alarjani and M. Alhaider, "A Review of Challenges of Block Chain with COVID-19: A Review Paper. European Journal of Health Sciences.," *European Journal of Health Sciences.*, vol. 8, no. 2, pp. 32-49, 2023.
- [86] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi and Z. Tari, "Blockchain-based federated learning for securing internet of things: A comprehensive survey.," *ACM Computing Surveys.*, vol. 55, no. 9, pp. 1-43., 2023.
- [87] K. Zoughalian, J. Marchang and B. Ghita, "A blockchain secured pharmaceutical distribution system to fight counterfeiting.," *International Journal of Environmental Research and Public Health.*, vol. 19, no. 7, p. 4091, 2022.
- [88] M. Aslam, S. Jabbar, Q. Abbas, M. Albathan, A. Hussain and U. Raza, "Leveraging Ethereum Platform for Development of Efficient Tractability System in Pharmaceutical Supply Chain.," *Systems.*, vol. 11, no. 4, p. 202, 2023.
- [89] D. Komarasamy, M. K. Dharani, R. Thamilselvan and J. J. Hermina, "Challenges, Progress and Opportunities of Blockchain in Healthcare Data.," *In Healthcare 4.0. Chapman and Hall/CRC.*, pp. 111-130, 2022.
- [90] T. Alam, "Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges.," *Computers.*, vol. 12, no. 1, p. 6, 2022.
- [91] S. A. Yousiff and R. A. A. H. Muhajir, "A Review of Blockchain-based Internet of Things. development, 6, 8.," *development. DOI: 10.37917/ijeee.19.1.3*, vol. 6, no. 8, 2022.
- [92] A. K. Yadav and V. P. Vishwakarma, "Adoption of Blockchain of Things (BCOT): Oppurtunities & Challenges.," *In 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS). IEEE.*, pp. 1-5, 2022.
- [93] S. Lipsa, T. N. Nguyen and R. K. Dash, "A New Signature-Based Blockchain Paradigm: Foreseeable Impact on Healthcare Applications," *IEEE Internet of Things Magazine.*, vol. 5, no. 3, pp. 146-151, 2022.
- [94] A. Razzaq, S. A. H. Mohsan, S. A. K. Ghayyur, N. Al-Kahtani, H. K. Alkahtani and S. M. Mostafa, "Blockchain in Healthcare: A Decentralized Platform for Digital Health Passport of COVID-19 Based on Vaccination and Immunity Certificates," *In Healthcare. MDPI.*, vol. 12, p. 10, 2453.
- [95] M. H. Yekta, A. Shahidinejad and M. Ghobaei-Arani, "Blockchain for transparent, privacy preserved, and secure health data management.," *In Implementation of Smart Healthcare Systems using AI, IoT, and Blockchain. Academic Press.*, pp. 219-242, 2023.
- [96] A. B. Tello, J. Xing, A. L. Patil, L. P. Patil and S. Sayyad, "Blockchain Technologies in Healthcare System for Real Time Applications Using IoT and Deep Learning Techniques.," *International Journal of Communication Networks and Information Security.*, vol. 14, no. 3, pp. 257-268, 2023.

- [97] S. S. Nath, S. Sadagopan, D. V. Babu, R. D. Kumar, P. Jonnala and M. Y. B. Murthy, "Block chain-based security and privacy framework for point of care health care IoT devices.," *Soft Computing.*, pp. 1-13., 2023.
- [98] M. Mejri, "HealthBlock: A Modular Framework for a Collaborative Sharing of Electronic Health Records Based on Blockchain.," <https://doi.org/10.21203/rs.3.rs-1881776/v1>, 2022.
- [99] G. M. Karthik, A. S. Kalyana Kumar, A. B. Karri and N. P. Jagini, "Deep intelligent blockchain technology for securing IoT-based healthcare multimedia data. Wireless Networks.," *Wireless Networks.*, pp. 1-13., 2023.
- [100] A. Hasselgren, K. Kravetska, D. Gligoroski, S. A. Pedersen and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review.," *International Journal of Medical Informatics.*, vol. 134, p. 104040., 2020.
- [101] D. Marbough, M. C. E. Simsekler, K. Salah, R. Jayaraman and S. Ellahham, "A Blockchain-Based Regulatory Framework for mHealth.," *Data.*, vol. 7, no. 12, p. 177, 2022.
- [102] A. E. Smail and F. Harmali, "Electronic Health Record (EHR) Management Blockchain-Based in Healthcare Systems.," *Doctoral dissertation, universit  akli mohand oulhadj-bouira.*, 2022.
- [103] K. Pal, "A Decentralized Privacy Preserving Healthcare Blockchain for IoT, Challenges, and Solutions.," *In Prospects of Blockchain Technology for Accelerating Scientific Advancement in Healthcare. IGI Global.*, pp. 158-188, 2022.
- [104] B. Balusamy, N. Chilamkurti, L. A. Beena and T. Poongodi, "Blockchain and machine learning for e-healthcare systems. Blockchain and Machine Learning for e-Healthcare Systems.," *Blockchain and Machine Learning for e-Healthcare Systems.*, pp. 1-481, 2021.
- [105] J. Zhang, "How do trust and decentralization impact adoption?: an agent-based model for diffusion of blockchain-based COVID-19 contact tracing apps.," *Doctoral dissertation, University of British Columbia.*, 2023.
- [106] S. Meisami, S. Meisami, M. Yousefi and M. R. Aref, "Combining Blockchain and IOT for Decentralized Healthcare Data Management.," *arXiv preprint arXiv.*, p. 2304.00127., 2023.
- [107] S. Gupta, M. Shabaz, A. Gupta, A. Alqahtani, S. Alsubai and I. Ofori, "Personal HealthCare of Things: A novel paradigm and futuristic approach.," *CAAI Transactions on Intelligence Technology.*, p. <https://doi.org/10.1049/cit2.12220>, 2023.
- [108] I. Azogu, A. Norta, I. Papper, J. Longo and D. Draheim, "A framework for the adoption of blockchain technology in healthcare information management systems: A case study of Nigeria.," *In Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance.*, pp. 310-316, 2019.
- [109] K. Pal, "Pal, K. (2023). Blockchain With the Internet of Things for Secure Healthcare Service Using Lightweight Cryptography.," *In Blockchain Applications in Cryptocurrency for Technological Evolution. IGI Global.*, pp. 60-93, 2023.
- [110] L. Javed, B. M. Yakubu, M. Waleed, Z. Khaliq, A. B. Suleiman and N. G. Mato, "A Survey on Healthcare IoT Security Issues and Blockchain-Based Solution.," *International Journal of Electrical and Computer Engineering Research.*, vol. 2, no. 4, pp. 1-9., 2022.
- [111] X. Yang, C. Wu, X. Yan and F. Hu, "Blockchain-Based Healthcare and Medicine Data Sharing and Service System.," in *In Blockchain and Trustworthy Systems: 4th International Conference, BlockSys (pp. 79-90).*2022, Singapore: Springer Nature Singapore, August 4–5, 2022. .
- [112] A. Pattanayaka and S. Dhala, "Blockchain in Healthcare.," *aComputer Science and Engineering Department, IIIT Guwahati, Assam, India*, 2021.
- [113] B. Sharma, "Blockchain: Remaking the Healthcare Sector.," *In 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART). IEEE.*, pp. 779-785, 2022.
- [114] L. Abdelgalil and M. Mejri, "HealthBlock: A Framework for a Collaborative Sharing of Electronic Health Records Based on Blockchain.," *Future Internet.*, vol. 15, no. 3, p. 87, 2023.
- [115] A. Tiwari and U. Batra, "Internet of Medical Things Enabled by Permissioned Blockchain on Distributed Storage.," *In International Conference on IoT, Intelligent Computing and Security. Springer, Singapore.*, pp. 3-17, 2023.
- [116] S. Showkat and S. Qureshi, "Securing the Internet of Things Through Blockchain Approach: Security Architectures, Consensus Algorithms, Enabling Technologies, Open Issues, and Research Directions.," *International Journal of Computing and Digital Systems.*, vol. 13, no. 1, pp. 97-129, 2023.
- [117] S. Chentharu, K. Ahmed, H. Wang, F. Whittaker and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology.," *Plos One.*, vol. 15, no. 12, p. e0243043., 2020.
- [118] S. Biswas, K. Sharif, F. Li, A. K. Bairagi, Z. Latif and S. P. Mohanty, "Globechain: An interoperable blockchain for global sharing of healthcare data—a covid-19 perspective.," *IEEE Consumer Electronics Magazine.*, vol. 10, no. 5, pp. 64-69., 2021.
- [119] K. Pal, "IoT Applications With Cryptography and Blockchain Technology in Healthcare Digital Twin Design.," *In Role of 6G Wireless Networks in AI and Blockchain-Based Applications. IGI Global.*, pp. 220-249, 2023.
- [120] O. Hasan, L. Brunie and E. Bertino, "Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey.," *ACM Computing Surveys (CSUR).*, vol. 55, no. 2, pp. 1-37, 2022.

- [121] N. Rifi, N. Agoulmine, N. Chendeb Taher and E. Rachkidi, "Blockchain technology: is it a good candidate for securing iot sensitive medical data?," *Wireless Communications and Mobile Computing*, 2018.
- [122] F. I. Anik, N. Sakib, H. Shahriar, Y. Xie, H. A. Nahiyani and S. I. Ahamed, "Unraveling a blockchain-based framework towards patient empowerment: A scoping review envisioning future smart health technologies.," *Smart Health*, p. 100401., 2023.
- [123] Y. Liu, F. Ju, Q. Zhang, M. Zhang, Z. Ma, M. Li, .. A. Yank and F. Liu, "Overview of Internet of Medical Things Security Based on Blockchain Access Control.," *Journal of Database Management (JDM)*, vol. 34, no. 3, pp. 1-20, 2023.
- [124] B. B. Sezer, H. Turkmen and U. Nuriyev, "PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks.," *Internet of Things*, p. 100781., 2023.
- [125] S. Uppal, B. Kansekar, S. Mini and D. Tosh, "HealthDote: A blockchain-based model for continuous health monitoring using interplanetary file system.," *Healthcare Analytics*, p. 100175, 2023.
- [126] P. Bedi, S. B. Goyal, J. Kumar and A. S. Rajawat, "Secure Medical Data Transmission Over Wireless Body Area Network Using Blockchain.," *In AI-Enabled Multiple-Criteria Decision-Making Approaches for Healthcare Management. IGI Global*, pp. 70 - 84, 2022.
- [127] H. K. Sharma, A. Kumar and S. R. M. Pant, "Artificial Intelligence, Blockchain and IoT for Smart Healthcare.," *CRC Press*, 2022.
- [128] S. Baskar and P. V. Gopirajan, "Application of Blockchain in Digital Healthcare.," *In 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE).IEEE*, pp. 591-595, 2023.
- [129] H. B. Mahajan and A. A. Junnarkar, "Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing.," *Multimedia Tools and Applications*, pp. 1 -24, 2023.
- [130] S. Shree, C. Zhou and M. Barati, "Data Protection in Internet of Medical Things Using Blockchain and Secret Sharing Method.," *Research Square -preprint*, no. <https://doi.org/10.21203/rs.3.rs-2791374/v1>, 2023.
- [131] N. K. Dewangan and P. Chandrakar, "TempChain: a blockchain scheme for telehealth data sharing between two blockchains using property mapping function.," *The Journal of Supercomputing*, pp. 1 -19, 2023.
- [132] A. Ali, M. F. Pasha, O. H. Fang, R. Khan, M. A. Almaiah and A. K. Al Hwaitat, "Big Data Based Smart Blockchain for Information Retrieval in Privacy-Preserving Healthcare System.," *In Big Data Intelligence for Smart Applications .Cham: Springer International Publishing*, pp. 279-296, 2022.
- [133] N. Lefkowitz and K. Boeckl, "NIST Privacy Framework: An Overview.," 2020. [Online]. Available: <https://tsapps.nist.gov/publication/getpdf.cfm?pub id=930470>. [Accessed 28 February 2021].
- [134] S. Mazumdar and T. Dreiholz, "Secure Embedded Living: Towards A Self-Contained User Data Preserving Framework.," *IEEE Communications Magazine*, vol. 60, no. 11, pp. 74 -80, 2022.
- [135] G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y. A. de Montjoye and A. Bourka, "Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics.," *arXiv preprint arXiv:1512.06000*, 2015.
- [136] C. Lee, L. Zappaterra, K. Choi and H. A. Choi, "Securing smart home: Technologies, security challenges, and security requirements.," *In 2014 IEEE Conference on Communications and Network Security*, pp. 67 -72, 2014.
- [137] Z. Zeng, Y. Li, Y. Cao, Y. Zhao, J. Zhong, D. Sidorov and X. Zeng, "Blockchain technology for information security of the energy internet: fundamentals, features, strategy and application.," *Energies*, vol. 13, no. 4, p. 881, 2020.
- [138] S. S. Dhanda, B. Singh and P. Jindal, "Lightweight cryptography: A solution to secure IoT.," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1947-1980, 2020.
- [139] R. Kamal, Internet of Things: Architecture and Design principles, TMH, India: ISBN-13: 978-93-525260-522-4, 2017, p. 403.
- [140] N. Guhr, O. Werth, P. P. H. Blacha and M. H. Breitner, "Privacy concerns in the smart home context.," *SN Applied Sciences*, vol. 2, no. 2, pp. 1 - 12, 2020.
- [141] E. COMMISSION, "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses," 25 January 2012. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46. [Accessed 20 March 2021].
- [142] Rt.com., "President Obama Announces Initiatives on Data Security and Student Privacy," 12 January 2015. [Online]. Available: <https://www.huntonprivacyblog.com/2015/01/12/president-obama-announces-initiatives-data-security-student-privacy/>. [Accessed 20 March 2021].
- [143] IEEE, "INTERNET OF THINGS (IOT) SECURITY BEST PRACTICE," IEEE Internet Technology Policy Community White Paper, 2017.
- [144] J. Wolff, "At Long Last, a Sensible Internet of Things Security Bill Has Been Introduced in the Senate," 3 August 2017. [Online]. Available: http://www.slate.com/blogs/future_tense/2017/08/03/the_senate_is_considering_an_internet_of_things_security_bill.html. [Accessed 12 January 2018].
- [145] C. Wirth and M. Kolain, "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data," *In Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET)*, 2018.

- [146] H. Rahanu, E. Georgiadou, K. Siakas, M. Ross and E. Berki, "Ethical issues invoked by Industry 4.0.," *In European Conference on Software Process Improvement. Springer, Cham.*, pp. 589 - 606, 2021.
- [147] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," *Trials*, vol. 18, no. 1, pp. 1-5, 2017.
- [148] M. Benchoufi, R. Porcher and P. Ravaud, "Blockchain protocols in clinical trials: Transparency and traceability of consent," *F1000Research*, p. 6, 2017.
- [149] T. Nugent, D. Upton and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts.," *F1000Research*, p. 5., 2016.
- [150] P. Pirzada, A. Wilde, G. H. Doherty and D. Harris-Birtill, "Ethics and acceptance of smart homes for older adults.," *Informatics for Health and Social Care.*, vol. 47, no. 1, pp. 10 - 37, 2022.
- [151] C. Wirth and M. Kolain, "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data.," *In Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET).*, 2018.
- [152] S. Al Salami, J. Baek, K. Salah and E. Damiani, "Lightweight encryption for smart home," *In 2016 11th International Conference on Availability, Reliability and Security (ARES) IEEE*, pp. 382-388, 2016.
- [153] M. A. Rodrigues and M. M. Siddeq, "Information System: Secure Access and Storage in the Age of Cloud Computing," *Athens Journal of Sciences*, vol. 3, no. 4, pp. 267-284, 2016.
- [154] G. S. Poh, P. Gope and J. Ning, "PrivHome: Privacy-preserving authenticated communication in smart home environment.," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1095 -1107, 2019.
- [155] M. Rodrigues, "AI Deep Learning and Data Security in the Internet of Everything," in *Kelaniya International Conference on Advances in Computing and Technology KICACT*, Colombo, Sri Lanka, 2016.
- [156] S. Lee, J. Choi, J. Kim, B. Cho, S. Lee, H. Kim and J. Kim, "FACT: Functionality-centric access control system for IoT programming frameworks.," *In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies.*, pp. 43-54, 2017.
- [157] F. Jonsson and M. Tornkvist, "RSA authentication in Internet of Things: Technical limitations and industry expectations.," <http://www.diva-portal.org/smash/get/diva2:1112039/FULLTEXT01.pdf>, Stockholm, Sweden , 2017.
- [158] K. Pal, "Blockchain With the Internet of Things for Secure Healthcare Service Using Lightweight Cryptography.," *In Blockchain Applications in Cryptocurrency for Technological Evolution. IGI Global.*, pp. 60 -93, 2023.
- [159] R. Wang, J. He, C. Liu, Q. Li, W. T. Tsai and E. Deng, "A privacy-aware PKI system based on permissioned blockchains.," *In 2018 IEEE 9th international conference on software engineering and service science (ICSESS).IEEE.*, pp. 928-931, 2018.
- [160] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan and M. Dasgupta, " A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *The Journal of Supercomputing*, vol. 77, no. 2, pp. 1114-1151, 2021.
- [161] R. Creaney, L. Reid and M. Currie, "The contribution of healthcare smart homes to older peoples' wellbeing: A new conceptual framework.," *Wellbeing, Space and Society.*, vol. 2, p. 100031, 2021.
- [162] S. Pesaru, N. K. Mallenahalli and B. V. Vardhan, "Light weight cryptography-based data hiding system for Internet of Medical Things.," *International Journal of Healthcare Management.*, pp. 1-14, 2022.
- [163] W. Yáñez, R. Bahsoon, Y. Zhang and R. Kazman, "Architecting internet of things systems with blockchain: A catalog of tactics.," *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 30, no. 3, pp. 1-46, 2021 .
- [164] W. Yáñez, R. Mahmud, R. Bahsoon, Y. Zhang and R. Buyya, "Data allocation mechanism for Internet-of-Things systems with BlockChain.," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3509-3522, 2020.
- [165] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home.," *In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* , pp. 618-623, 2017.
- [166] Q. Wang, T. Xia, Y. Ren, L. Yuan and G. Miao, " A New Blockchain-Based Multi-Level Location Secure Sharing Scheme.," *Applied Sciences*, vol. 11, no. 5, p. 2260, 2021.
- [167] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar and K. K. R. Choo, "HomeChain: A blockchain-based secure mutual authentication system for smart homes.," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 818-829, 2019.
- [168] Alpa, "Proof-of-Authority consensus," 2018. [Online]. Available: <https://apla.readthedocs.io/en/latest/concepts/consensus.html>. [Accessed 10 October 2021].
- [169] G. Zyskind and O. Nathan, " Decentralizing privacy: Using blockchain to protect personal data.," *In 2015 IEEE Security and Privacy Workshops. IEEE.*, pp. 180-184, 2015.
- [170] D. Schreckling, J. D. Parra, C. Doukas and J. Posegga, "Data-Centric Security for the IoT," *In International Internet of Things Summit, Springer, Cham.*, pp. 77-86, 2015.

- [171] A. Outchakoucht, E. Hamza and J. Leroy, "Dynamic access control policy based on blockchain and machine learning for the internet of things.," *International journal of advanced Computer Science and applications.*, vol. 8, no. 7, pp. 417-424, 2017.
- [172] W. Han, Y. Zhang, Z. Guo and E. Bertino, "Fine-grained business data confidentiality control in cross-organizational tracking.," *In Proceedings of the 20th ACM Symposium on Access Control Models and Technologies.*, pp. 135 -145, 2015.
- [173] P. Zhong, Q. Zhong, H. Mi, S. Zhang and Y. Xiang, "Privacy-protected blockchain system.," *In 2019 20th IEEE International Conference on Mobile Data Management (MDM) IEEE.*, pp. 257 - 461, 2019.
- [174] R. Almadhoun, M. Kadadha and M. Alhemeiri, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes.," *In 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA)IEEE.*, pp. 1-8, 2018.
- [175] S. Namasudra, S. Nath and A. Majumder, " Profile based access control model in cloud computing environment.," *In 2014 International Conference on Green Computing Communication and Electrical Engineering*, pp. 1-5, 2014.
- [176] Q. Wang, T. Xia, Y. Ren, L. Yuan and G. Miao, " A New Blockchain-Based Multi-Level Location Secure Sharing Scheme.," *Applied Sciences.*, vol. 11, no. 5, p. 2260, 2021.
- [177] N. Rifi, N. Agoulmine, N. Chendeb Taher and E. Rachkidi, "Blockchain technology: is it a good candidate for securing iot sensitive medical data?," *Wireless Communications and Mobile Computing.*, 2018.
- [178] W. River, "Security in the Internet of Things: Lessons from the Past for the Connected Future.," *WIND River.*, 2015.
- [179] T. Hardjono, "Kerberos for Internet-of-Things," MIT Kerberos & Internet Trust Consortium, IETF89, February 2014. [Online]. Available: ". URL: <http://www.tschofenig.priv.at/tutorials/Kerberos-Tutorial.pdf> (abgerufen am 08.06. 2015), 25.. [Accessed 13 February 2020].
- [180] H. Kim, A. Wasicek, B. Mehne and E. A. Lee, "A secure network architecture for the internet of things based on local authorization entities," *016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE*, pp. 114-122, August, 2016.
- [181] H. Kim and E. A. Lee, "Trusting the Internet of Things: Authentication and Authorization for the Internet of Things," *IT Professional*, vol. 19, no. 5, pp. 27-33, 2017.
- [182] W. He, V. Zhao, O. Morkved, S. Siddiqui, E. Fernandes, J. Hester and B. Ur, "SoK: Context sensing for access control in the adversarial home IoT.," *In 2021 IEEE European Symposium on Security and Privacy (EuroS&P)* , pp. 37-53, 2021.
- [183] N. Ghosh, S. Chandra, V. Sachidananda and Y. Elovici, " SoftAuthZ: a context-aware, behavior-based authorization framework for home IoT.," *IEEE Internet of Things Journal.*, vol. 6, no. 6, pp. 10773-10785., 2019.
- [184] A. S. J. Ukil and S. Koilakonda, "Embedded security for Internet of Things," *In 2011 2nd National Conference on Emerging Trends and Applications in Computer Science. IEEE.*, pp. 1-6, 2011.
- [185] H. HaddadPajouh, R. Khayami, A. Dehghantanha, K. K. R. Choo and R. M. Parizi, "AI4SAFE-IoT: An AI-powered secure architecture for edge layer of Internet of things.," *Neural Computing and Applications*, , vol. 32, no. 20, pp. 16119-16133., 2020.
- [186] I. Psychoula, "Privacy Modelling and Preservation for Assisted Living within Smart Homes.," DeMortfort University, Leicester, 2020.
- [187] A. Verma, K. Sahay, S. Prakash, A. Kumar, A. Kumar, H. F. M. Lahza, H. Lahza and M. A. Albahar, "A Systematic Review on Machine Learning Fundamentals for Smart Home.," *Towards Smart City Solution.*, 2023.
- [188] K. P. M. T. Revathi, " A Smart and Secured Approach for Children's Health Monitoring Using Machine Learning Techniques Enhancing Data Privacy.," *IETE Journal of Research.*, pp. 1 - 12, 2022.
- [189] M. M. Salim, L. Park and J. H. Park, " A Machine Learning based Scalable Blockchain architecture for a secure Healthcare system.," *In 2022 13th International Conference on Information and Communication Technology Convergence (ICTC).IEEE*, pp. 2231-2234, 2022.
- [190] G. Vellyyangiri, V. Krishnamoorthy, C. Inbaraj, A. Venkatachalam, R. Rahim and M. Ramachandran, "Blockchain and Artificial Intelligent for Internet of Things in e-Health.," *In The Convergence of Artificial Intelligence and Blockchain Technologies: Challenges and Opportunities.*, pp. 23-42, 2022.
- [191] J. Mandala, R. Ganeshan, B. Maram and T. Daniya, "IoT and Artificial Intelligence for Healthcare Informatics: Evolving Technologies.," *In Handbook of Research on Mathematical Modeling for Smart Healthcare Systems IGI Global.*, pp. 110-120, 2022.
- [192] H. K. Sharma, A. Kumar, S. Pant and M. Ram, "Artificial Intelligence, Blockchain and IoT for Smart Healthcare.," *CRC Press*, 2022.
- [193] R. Kumar, D. Singh, K. Srinivasan and Y. C. Hu, "AI-Powered Blockchain Technology for Public Health: A Contemporary Review, Open Challenges, and Future Research Directions.," *In Healthcare. MDPI.*, vol. 11, no. 1, p. 81, 2022.
- [194] C. Pirtle and J. Ehrenfeld, "Blockchain for healthcare: The next generation of medical records?," *Journal of Medical Systems*, vol. 42, no. 9, pp. 1-3, 2018.

- [195] K. Farooq, H. J. Syed, S. O. Alqahtani, W. Nagmeldin, A. O. Ibrahim and A. Gani, "Blockchain Federated Learning for In-Home Health Monitoring. Electronics.," *Electronics.*, vol. 12, no. 1, p. 136, 2022.
- [196] V. K. Prasad, P. Bhattacharya, D. Maru, S. Tanwar, A. Verma, A. Singh, A. Tiwari, R. Sharma, A. Alkhayyat, F. Țurcanu and M. S. Raboaca, "Federated Learning for the Internet-of-Medical-Things: A Survey.," *Mathematics.*, vol. 11, no. 1, p. 151, 2022.
- [197] A. A. Alzahrani, "Using Artificial Intelligence and Cybersecurity in Medical and Healthcare Applications.," Alzahrani, A. A. (2023). Using Artificial Intelligence and Cybersecurity in Medical and Healthcare Applications. 2023.
- [198] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai and D. Trentesaux, "A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0.," *Sustainability*, vol. 12, no. 21, p. 9179, 2020.
- [199] K. Hameed, M. Barika, S. Garg, M. B. Amin and B. Kang, "A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues.," *Journal of Industrial Information Integration*, vol. 26, no. 1, p. 100312., 2022.
- [200] M. Alwabe and Y. Kwon, "Blockchain Consistency Check Protocol for Improved Reliability.," *Computer Systems Science & Engineering.*, vol. 36, no. 2, 2021.
- [201] D. Cocîrlea, C. Dobre, L. A. Hîrțan and R. Purnichescu-Purtan, "Blockchain in intelligent transportation systems," *Electronics*, vol. 9, no. 10, p. 1682, 2020.
- [202] A. S. Bale, T. P. Purohit, M. F. Hashim and S. Navale, "Blockchain and Its Applications in Industry 4.0.," *A Roadmap for Enabling Industry 4.0 by Artificial Intelligence*, pp. 295-313, 2022.
- [203] A. O. Almagrabi, R. Ali, D. Alghazzawi, A. AlBarakati and T. Khurshaid, "Blockchain-as-a-Utility for Next-Generation Healthcare Internet of Things.," *Computers, Materials & Continua*, vol. 68, no. 1, 2021.
- [204] Q. Wang, R. Li and L. Zhan, "Blockchain technology in the energy sector: From basic research to real world applications," *Computer Science Review*, vol. 39, p. 100362, 2021.
- [205] VeChain, "VeChain Whitepaper 2.0," VeChain Foundation, http://www.vechain.org/qfy-content/uploads/2020/01/VeChainWhitepaper_2.0_en.pdf, 2019.
- [206] VeChain, "VeChain Whitepaper 2.0 - Creating Valuable TXs on The VeChainThor Blockchain," VeChain Foundation, 12 2019. [Online]. Available: https://www.vechain.org/whitepaper/#bit_65sv8. [Accessed 2 December 2021].
- [207] D. Das, S. Banerjee, U. Ghosh, U. Biswas and A. K. Bashir, "A decentralized vehicle anti-theft system using Blockchain and smart contracts," *Peer-to-Peer Networking and Applications*, pp. 1 - 14, 2021.
- [208] J. M. N. T. P. Karamachoski, "Blockchain-based application for certification management.," *Tehnički glasnik.*, vol. 14, no. 4, pp. 488-492, 2020.
- [209] Paradigm, "ICON: Detailed review on the project," 8 November 2018. [Online]. Available: <https://medium.com/paradigm-research/icon-detailed-review-on-the-project-2efd550779ff>. [Accessed 18 August 2023].
- [210] I. Foundation, "icon Hypeconnect the world," 15 August 2017. [Online]. Available: <http://docs.icon.foundation/ICON-Whitepaper-EN-Draft.pdf>. [Accessed 18 August 2023].
- [211] J. Jeong, "AWS Partner Case Study: ICONLOOP," [Online]. Available: <https://aws.amazon.com/partners/success/iconloop/>. [Accessed 18 August 2023].
- [212] R. Doshi, "Blockchain Adoption Journey and Impact on Financial Services Industry," [Online]. Available: <https://www.infosys.com/insights/ai-automation/blockchain-adoption-journey.html>. [Accessed 18 August 2023].
- [213] K. Gaikwad, K. Kulkarni, S. Kohle and P. Patil, "Implementation of Blockchain Technology in IOT Based Smart Home.," *In 2022 5th International Conference on Advances in Science and Technology (ICAST). IEEE.*, pp. 6-10, 2022.
- [214] A. D. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT.," *Sensors.*, vol. 19, no. 2, p. 326., 2019.
- [215] S. K. Rana, A. K. Rana and S. Dhawan, "A Vital Fusion of Internet of Medical Things and Blockchain to Transform Data Privacy and Security.," in *Convergence of Deep Learning and Artificial Intelligence in Internet of Things*, CRC Press, 2022, pp. 293 - 308.
- [216] K. P. Satamraju, "Proof of concept of scalable integration of internet of things and blockchain in healthcare.," *Sensors.*, vol. 20, no. 5, p. 1389, 2020.
- [217] C. Ploder, T. Spiess, R. Bernsteiner, T. Dilger and R. Weichelt, "A risk analysis on blockchain technology usage for electronic health records," *Cloud Computing and Data Science*, pp. 20-35, 2021.
- [218] R. Pathak, B. Soni and N. B. Muppalaneni, "Role of Blockchain in Health Care: A Comprehensive Study.," in *In Proceedings of 3rd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications: ICMISC*, Singapore: Springer Nature Singapore., 2023.
- [219] B. Sharma, "Blockchain: Remaking the Healthcare Sector.," *In 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART) . IEEE.*, pp. 779-785, 2022.
- [220] S. S. Nath, S. Sadagopan, D. V. Babu, R. D. Kumar, P. Jonnala and M. Y. B. Murthy, "Block chain-based security and privacy framework for point of care health care IoT devices.," *Soft Computing.*, pp. 1-13., 2023.

- [221] D. Yonathan, D. Husna, F. A. Ekadiyanto, I. K. E. Purnama, A. N. Hidayati, M. H. Purnomo, S. Nugroho, R. Rachmadi, I. Nurtanio and A. A. P. Ratna, "Design of decentralized application for telemedicine image record system with smart contract on ethereum.," *International Journal of Advanced Computer Science and Applications.*, vol. 12, no. 10, 2021.
- [222] L. Abdelgalil and M. Mejri, "HealthBlock: A Framework for a Collaborative Sharing of Electronic Health Records Based on Blockchain.," *Future Internet.*, vol. 15, no. 3, p. 87, 2023.
- [223] A. D. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT.," *Sensors.*, vol. 19, no. 2, p. 326, 2019.
- [224] B. S. Egala, A. K. Pradhan, P. Dey, V. Badarla and S. P. Mohanty, "Fortified-Chain 2.0: Intelligent Blockchain for Decentralized Smart Healthcare System.," *IEEE Internet of Things Journal.*, 2023.
- [225] M. Paul, L. Maglaras, M. A. Ferrag and I. AlMomani, "Digitization of healthcare sector: A study on privacy and security concerns.," *ICT Express.*, 2023.
- [226] Z. Ilyas, M. I. Tariq, S. K. Shahzad and R. A. Karim, "Resolving Smart Health Security Issues Using Ontologies and Blockchain Services.," *PAKISTAN JOURNAL OF EMERGING SCIENCE AND TECHNOLOGIES (PJEST)*, vol. 3, no. 2, 2023.
- [227] A. Ekblaw, A. Azaria, J. D. Halamka and A. Lippman, "A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data.," . In *Proceedings of IEEE open & big data conference*, vol. 13, p. 13, Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13, p. 13). Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13, p. 13). 2016 .
- [228] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research.," in *In ONC/NIST use of blockchain for healthcare and research workshop.* , Gaithersburg, Maryland, United States, 2016.
- [229] S. Tiwari, D. N. and H. Dev, "An Intelligent Healthcare Framework for Data Security Based on Blockchain and Internet of Things.," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10, no. 3, pp. 95-102, 2022.
- [230] A. Lekssays, G. Sirigu, B. Carminati and E. Ferrari, "MalRec: A Blockchain-based Malware Recovery Framework for Internet of Things.," *In Proceedings of the 17th International Conference on Availability, Reliability and Security.*, pp. 1-8, 2022.
- [231] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi and K. L. Tan, "Blockbench: A framework for analyzing private blockchains.," *In Proceedings of the 2017 ACM international conference on management of data.*, pp. 1085-1100, 2017.
- [232] B. Wang and Z. Li, "Healthchain: A Privacy Protection System for Medical Data Based on Blockchain.," *Future Internet.*, vol. 13, no. 10, p. 247, 2021.
- [233] A. Raj and S. Prakash, " Smart Contract-Based Secure Decentralized Smart Healthcare System.," *International Journal of Software Innovation (IJSI)*, vol. 11, no. 1, pp. 1-20., 2023.
- [234] T. L. N. Dang and M. S. Nguyen, "An approach to data privacy in smart home using blockchain technology.," *In 2018 International Conference on Advanced Computing and Applications (ACOMP)*, pp. 58-64, 2018.
- [235] S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. K. Lakshmanaprabu and A. Khanna, "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy.," *Future Generation Computer Systems.*, vol. 102, pp. 1027-1037, 2020.
- [236] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity.," *Journal of Parallel and Distributed Computing.*, vol. 134, pp. 180-197., 2019.
- [237] A. Qashlan, P. Nanda, X. He and M. Mohanty, "Privacy-preserving mechanism in smart home using blockchain.," *Privacy-preserving mechanism in smart home using blockchain. IEEE Access.*, vol. 9, pp. 103651-103669., 2021.
- [238] K. Azbeg, O. Ouchetto and S. J. Andaloussi, "Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management.," *IEEE Transactions on Computational Social Systems.*, 2022.
- [239] O. Hasan, L. Brunie and E. Bertino, "Privacy-Preserving Reputation Systems Based on Blockchain and Other Cryptographic Building Blocks: A Survey.," *ACM Computing Surveys (CSUR)*, vol. 55, no. 2, pp. 1 - 37, 2022.
- [240] H. J. Jo and W. Choi, "BPRF: Blockchain-based privacy-preserving reputation framework for participatory sensing systems.," *Plos one.*, vol. 14, no. 12, p. e0225688., 2019.
- [241] P. Sharma, S. Namasudra, N. Chilamkurti, B. G. Kim and R. Gonzalez Crespo, "Blockchain-based privacy preservation for IoT-enabled healthcare system," *ACM Transactions on Sensor Networks*, vol. 19, no. 3, pp. 1-17, 2023.
- [242] M. I. Ahmed, G. Kannan and S. R. Polamuri, "LSITA: An Integrated Framework for Leveraging Security of Internet of Things Application with Remote Patient Monitoring System.," *Research Square*, 2022.
- [243] S. Das, S. Namasudra, S. Deb, P. M. Ger and R. G. Crespo, "Securing IoT-based Smart Healthcare Systems by using Advanced Lightweight Privacy-Preserving Authentication Scheme," *IEEE Internet of Things Journal.*, 2023.

- [244] A. Buldas and A. L. R. Kroonmaa, "Keyless signatures' infrastructure: How to build global distributed hash-trees.," *In Nordic Conference on Secure IT System. Berlin, Heidelberg: Springer Berlin Heidelberg.*, pp. 313 - 320.
- [245] I. Allison, "Guardtime secures over a million Estonian healthcare records on the blockchain," 3 March 2012. [Online]. Available: <http://www.ibtimes.co.uk/guardtime-secures-over-millionestonian-healthcare-records-blockchain-1547367>. [Accessed 18 August 2023].
- [246] U. ALI, M. Y. I. B. IDRIS, J. O. FRNDA, M. N. B. AYUB, M. A. KHAN, N. KHAN, B. T. REHANNARA, A. JASIM, I. ULLAH and M. BABAR, "Enhanced Lightweight and Secure Certificateless Authentication Scheme (ELWSCAS) for Internet of Things Environment," *Internet of Things*, p. 100923, 2023.
- [247] O. Popoola and B. Pranggono, "On energy consumption of switch-centric data center networks.," *The Journal of Supercomputing.*, vol. 74, no. 1, pp. 334-369, 2018.
- [248] W. E. Forum, "The aviation sector wants to reach net zero by 2050. How will it do it?," 9 December 2022. [Online]. Available: <https://www.weforum.org/agenda/2022/12/aviation-net-zero-emissions/>. [Accessed 18 August 2023].
- [249] M. Lawford, "The industry more damaging to the environment than airlines," 30 May 2023 . [Online]. Available: <https://www.telegraph.co.uk/business/2023/05/30/silicon-valley-data-giants-net-zero-sustainability-risk/#:~:text=The%20world's%20computing%20and%20information,much%20electricity%20as%2050%2C000%20homes..> [Accessed 23 August 2023].
- [250] S. Namasudra and P. Sharma, "Achieving a decentralized and secure cab sharing system using blockchain technology.," *IEEE Transactions on Intelligent Transportation Systems.*, 2022.
- [251] S. Bansal and D. Kumar, "IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication.," *International Journal of Wireless Information Networks.*, vol. 27, no. 3, pp. 340 -364, 2020.
- [252] C. C. f. A. Finance, " Cambridge Bitcoin Electricity Consumption Index.," [Online]. Available: <https://ccaf.io/cbnsi/cbeci>. [Accessed 10 September 2023].
- [253] N. Radziwill, "Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world," *The Quality Management Journal*, vol. 25, no. 1, pp. 64-65, 2018.
- [254] M. J. Krause and T. Tolaymat, "Quantification of energy and carbon costs for mining cryptocurrencies," *Nature Sustainability*, vol. 1, no. 11, pp. 711-718, 2018.
- [255] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," *Hamilton Institute, Maynooth University*, 2014.
- [256] P. K. Singh, R. Singh and S. K. N. S. Nandi, "Managing smart home appliances with proof of authority and blockchain.," in *In Innovations for Community Services: 19th International Conference, I4CS 2019, June 24-26, 2019, Proceedings 19 (pp. 221-232). Springer International Publishing.*, Wolfsburg, Germany, 2019.
- [257] E. Karaarslan and E. Konacaklı, "Data storage in the decentralized world: Blockchain and derivatives.," *arXiv preprint arXiv:2012.*, p. 10253, 2020.
- [258] A. Brock, D. Atkinson, E. Friedman, E. Harris-Braun, E. McGuire, J. M. Russell, E. McGuire, J. Russell, N. Perrin, N. Luck and W. Harris-Braun, "Holo Green Paper," *Green Paper*, 2018.
- [259] C. Diallo, "Opportunities and Challenges of IoT Security Using Distributed Ledger Technology," *Sensors & Transducers*, vol. 256, no. 2, pp. 27-35, 2022.
- [260] A. Sasikumar, S. Vairavasundaram, K. Kotecha, V. Indragandhi, L. Ravi, G. Selvachandran and A. Abraham, "Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things.," *Future Generation Computer Systems*, vol. 141, pp. 16-27., 2023.
- [261] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi and M. Ishfaq, "Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing.," *Future Internet*, vol. 14, no. 11, p. 341, 2022.
- [262] S. S. Kamble, A. Gunasekaran and S. A. Gawankar, "Achieving sustainable performance in a data-driven agriculture supply chain: A review for research and applications," *International Journal of Production Economics*, vol. 219, pp. 179-194., 2020.
- [263] P. Woitschig, G. S. Uddin, T. Xie and W. K. Härdle, "The energy consumption of the ethereum-ecosystem," *Available at SSRN 4526732.*, 2023.
- [264] M. Crippa, E. Solazzo, D. Guizzardi, F. Monforti-Ferrario, F. N. Tubiello and A. J. N. F. Leip, " Food systems are responsible for a third of global anthropogenic GHG emissions," *Nature Food*, vol. 2, no. 3, pp. 198-209, 2021.
- [265] T. H. B. S. W. L. I. AlSkaif and W. Van Sark, "A blockchain-based configuration for balancing the electricity grid with distributed assets.," *World Electric Vehicle Journal*, vol. 11, no. 4, p. 62, 2020.
- [266] A. Lamba, "Are carbon offsets the key to green cryptocurrencies?," *PLOS Sustainability and Transformation*, vol. 1, no. 3, p. e0000002, 2022.
- [267] L. Belkhir and A. Elmeli, " Assessing ICT global emissions footprint: Trends to 2040 & recommendations," *Journal of cleaner production*, vol. 177, pp. 448-463, 2018.
- [268] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan and J. Yellick, "Hyperledger fabric: a distributed operating system for permissioned blockchains," *In Proceedings of the thirteenth EuroSys conference* , pp. 1 -15, 2018.
- [269] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, "Bitcoin and cryptocurrency technologies Princeton.," *Princeton University Press*, 2016.
- [270] E. B. O. a. Forum, "Energy Efficiency of Blockchain Technologies: A Thematic Report," [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/reports/Energy%20Efficiency%20of%20Blockchain%20Technologies_1.pdf. [Accessed 10 September 2023].

- [271] S. Gaba, H. Khan, K. J. Almalli, A. Jabbari, I. Budhiraja, V. Kumar, A. Singh, K. Singh, S. Askar and M. Abouhawwash, "Holochain: An Agent-Centric Distributed Hash Table Security in Smart IoT Applications.," *IEEE Access.*, 2023.
- [272] A. A. Kamran, I. U. Din, A. Almogren, A. K. Hasan and J. P. C. R. Joel, " EdgeTrust: A lightweight data-centric trust management approach for IoT-based healthcare 4.0.," *Electronics*, vol. 12, no. 1, p. 140, 2023.
- [273] A. Aftab, C. Chrysostomou, H. K. Qureshi and S. Rehman, "Holo-Block Chain: A Hybrid Approach for Secured IoT Healthcare Ecosystem.," *In 2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE*, pp. 243-250, 2022.
- [274] C. Zepeda-Lugo, D. Tlapa, Y. Baez-Lopez and J. Limon-Romero, "Critical factors of lean healthcare: an overview," *In Proceedings of the International Conference on Healthcare Service Management*, pp. 1-7, 2018.
- [275] S. Zaman, M. R. Khandaker, R. T. Khan, F. Tariq and K. K. Wong, "Thinking out of the blocks: Holochain for distributed security in iot healthcare," *IEEE Access.*, vol. 10, pp. 37064-37081, 2022.
- [276] K. Janjua, M. A. Shah, A. Almogren, H. A. Khattak, C. Maple and I. U. Din, " Proactive forensics in IoT: Privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies.," *Electronics*, vol. 9, no. 7, p. 1172, 2020.
- [277] A. D. Dwivedi, R. Singh, U. Ghosh, R. R. Mukkamala, A. Tolba and O. Said, "Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1 - 11, 2021.
- [278] T. Kuhrt, "Hyperledger Projects- Hyperledger Foundation," 3 January 2022. [Online]. Available: <https://wiki.hyperledger.org/display/TSC/Hyperledger+Projects>. [Accessed 12 January 2022].
- [279] R. Pandey, "How to measure your body composition on the Samsung Galaxy Watch 4 and Watch 5 series," 19 December 2022. [Online]. Available: <https://www.androidpolice.com/measure-body-composition-samsung-galaxy-watch/>. [Accessed 13 January 2023].
- [280] S. C. Mukhopadhyay, "Wearable sensors for human activity monitoring: A review.," *IEEE sensors journal*, vol. 15, no. 3, pp. 1321-1330., 2014.
- [281] S. Majumder, T. Mondal and M. J. Deen, "Wearable sensors for remote health monitoring.," *Sensors.*, vol. 17, no. 1, p. 130, 2017.
- [282] S. Bushwick, "'Anonymous' Data Won't Protect Your Identity," 23 July 2019. [Online]. Available: <https://www.scientificamerican.com/article/anonymous-data-wont-protect-your-identity/>. [Accessed 23 December 2021].
- [283] B. News, "Hackers steal \$600m in major cryptocurrency heist," 11 August 2021. [Online]. Available: <https://www.bbc.co.uk/news/business-58163917>. [Accessed 12 August 2021].
- [284] S. Venkataramakrishnan and P. Stafford, "Hackers siphon \$600m in digital tokens, crypto network says," 10 August 2021. [Online]. Available: <https://www.ft.com/content/47329261-afec-4cf7-840e-5eee0c70ba61>. [Accessed 12 August 2021].
- [285] L. Harley-McKeown, "Hackers begin returning funds from sensational \$600m crypto heist," 11 August 2021. [Online]. Available: <https://uk.news.yahoo.com/cryptocurrency-poly-network-hackers-return-funds-defi-ethereum-110935552.html?guccounter=1>. [Accessed 12 August 2021].
- [286] T. Robinson and A. Krishnakumar, "Institutions seek detailed blockchain analytics for crypto adoption — Elliptic," 28 May 2023. [Online]. Available: <https://cointelegraph.com/news/institutions-seek-detailed-blockchain-analytics-for-crypto-adoption-elliptic>. [Accessed 17 Septemeber 2023].
- [287] I. Docs, "How IPFS works," 7 December 2022., [Online]. Available: <https://docs.ipfs.tech/concepts/how-ipfs-works/#content-addressing>. [Accessed 9 January 2023].
- [288] E. Saleh and S. Rajesh, "High-performance cryptanalysis: a comparative study of code-breaking techniques.," in *In Proceedings of the International Conference on Innovative Computing & Communication (ICICC).*, 2021 .
- [289] G. Pedroza and P. Tessier, "D5.5 Methods for data protection and privacy model-driven design v2," ResearchGate, DOI: 10.13140/RG.2.2.30257.45929, 2020.
- [290] S. Becher, A. Gerl, B. Meier and F. Bölz, "Big picture on privacy enhancing technologies in e-health: a holistic personal privacy workflow. Information," *Information.*, vol. 11, no. 7, p. 356, 2020.
- [291] A. R. Sfar, E. Natalizio, S. Mazlout, Y. Challal and Z. Chtourou, "Privacy preservation using game theory in e-health application.," *Journal of information security and applications.*, vol. 66, p. 103158., 2022.

