Secure-by-Design Real-Time Internet of Medical Things Architecture: e-Health Population Monitoring (RTPM)

MARCHANG, Jims <http://orcid.org/0000-0002-3700-6671>, MCDONALD, Jade, KEISHING, Solan, ZOUGHALIAN, Kavyan, MAWANDA, Raymond, DELHON-BUGARD, Corentin, BOUILLET, Nicolas and SANDERS, Ben

Citation:

MARCHANG, Jims, MCDONALD, Jade, KEISHING, Solan, ZOUGHALIAN, Kavyan, MAWANDA, Raymond, DELHON-BUGARD, Corentin, BOUILLET, Nicolas and SANDERS, Ben (2024). Secure-by-Design Real-Time Internet of Medical Things Architecture: e-Health Population Monitoring (RTPM). Telecom, 5 (3), 609-631. [Article] telecom

MDPI

Article

Secure-by-Design Real-Time Internet of Medical Things Architecture: e-Health Population Monitoring (RTPM)

Jims Marchang [1,*], Jade McDonald [1], Solan Keishing [2], Kavyan Zoughalian [1], Raymond Mawanda [1], Corentin Delhon-Bugard [3], Nicolas Bouillet [3] and Ben Sanders [4]

[1] Computing Department and AWRC, Sheffield Hallam University, Sheffield S1 1WB, UK

[2] Computer Science and Engineering, National Institute of Technology, Manipur, Imphal 795004, India

[3] Graduate School of Science and Engineering, Junia, 59014 Lille, France; nicolas.bouillet@student.junia.com (N.B.)

[4] Department of Digital Futures, University of Winchester, Winchester S022 4NR, UK; ben.sanders@winchester.ac.uk

* Correspondence: jims.marchang@shu.ac.uk

Abstract: The healthcare sector has undergone a profound transformation, owing to the influential role played by Internet of Medical Things (IoMT) technology. However, there are substantial concerns over these devices' security and privacy-preserving mechanisms. The current literature on IoMT tends to focus on specific security features, rather than wholistic security concerning Confidentiality, Integrity, and Availability (CIA Triad), and the solutions are generally simulated and not tested in a real-world network. The proposed innovative solution is known as Secure-by-Design Real-Time IoMT Architecture for e-Health Population Monitoring (RTPM) and it can manage keys at both ends (IoMT device and IoMT server) to maintain high privacy standards and trust during the monitoring process and enable the IoMT devices to run safely and independently even if the server is compromised. However, the session keys are controlled by the trusted IoMT server to lighten the IoMT devices' overheads, and the session keys are securely exchanged between the client system and the monitoring server. The proposed RTPM focuses on addressing the major security requirements for an IoMT system, i.e., the CIA Triad, and conducts device authentication, protects from Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, and prevents non-repudiation attacks in real time. A self-healing solution during the network failure of live e-health monitoring is also incorporated in RTPM. The robustness and stress of the system are tested with different data types and by capturing live network traffic. The system's performance is analysed using different security algorithms with different key sizes of RSA (1024 to 8192 bits), AES (128 to 256 bits), and SHA (256 bits) to support a resource-constraint-powered system when integrating with resource-demanding secure parameters and features. In the future, other security features like intrusion detection and prevention and the user's experience and trust level of such a system will be tested.

Keywords: IoMT; IoT; patient health monitoring; secure monitoring; secure healthcare; RTPM

check for updates

Citation: Marchang, J.; McDonald, J.; Keishing, S.; Zoughalian, K.; Mawanda, R.; Delhon-Bugard, C.; Bouillet, N.; Sanders, B. Secure-by-Design Real-Time Internet of Medical Things Architecture: e-Health Population Monitoring (RTPM). *Telecom* **2024**, *5*, 609–631. https://doi.org/10.3390/telecom5030031

Academic Editor: Achilles Boursianis

Received: 4 June 2024
Revised: 27 June 2024
Accepted: 5 July 2024
Published: 10 July 2024

1. Introduction

Technology is ever-changing, and it has revolutionised the ways in which people are connected and things are monitored and controlled. Technological strides have touched every dimension of our daily lives, transforming the way we navigate transportation, conduct business, engage in marketing, manage our homes, and even approach healthcare. The advent of the Internet of Things (IoT) and akin technologies has ushered in a revolution, introducing captivating and innovative methods for monitoring things and surroundings, including monitoring patients in the realm of traditional and advanced healthcare systems. The introduction of high-speed data transmission and networking has allowed advancements in the domain of healthcare services as it allows better connectivity and monitoring [1]. Thus, sensors can now be deployed and utilised to monitor patients, allowing for timely and accurate diagnoses and immediate healthcare actions. It is important to note that this progress in monitoring has drastically improved the way patients can be cared for within the healthcare domain and, in turn, enhances their Quality of Life (QoL) because such a system allows live monitoring and provides scope for making decisions and actions in real-time.

1.1. Introduction Internet of Things (IoT)

The Internet of Things (IoT) has transformed the way objects are monitored and data are collected over a network [2]. It allows us to connect and monitor things locally and remotely. The IoT has empowered systems for automatic data collection rather than depending on human participation during its process. Generally, humans are error-prone and are highly inefficient in comparison to computing systems, especially in the field of data collection. IoT's application is now widespread, and it is seen in various fields, including smart healthcare, smart homes, automated supply chain management systems, remote environmental monitoring, smart city monitoring, etc. The IoT leverages machine-to-machine (M2M) communication, replacing the need for humans to provide data input, which ensures scalability, reliability, and accuracy. The IoT has a significant advantage because of its interoperability with many existing systems and networks. It is transforming healthcare applications, and such IoT systems that are used in medical-related monitoring and control are termed the Internet of Medical Things (IoMT).

1.2. Internet of Medical Things (IoMT)

IoT healthcare devices, also referred to as the Internet of Medical Things (IoMT), are IoT devices specifically created for healthcare purposes. Examples of this can be remote patient monitoring, home or hospital patient monitoring, pacemaker implants, wearable devices, diabetes sensors, and others. The IoMT is transforming patient treatment, enhancing the potential for successful patient recovery. The IoMT can improve QoL, prolong life expectancies, provide real-time patient data, directly impact patient health with faster reactions from doctors or nurses, and much more [3]. In recent times, the adoption of IoMT devices has extensively escalated. The utilisation of IoMT is on the rise, with current trends pointing toward increased adoption of these devices. The applications of the IoMT are growing: IoMT revenue in 2017 was USD 28 billion, and it is expected to grow to USD 135 billion by 2025 [4]; a similar report about the growing popularity of IoMT applications is also available in [5]. The IoMT consists of a network system with two primary components: local monitoring and remote monitoring. IoMT devices used for local monitoring can be defined by any IoMT system operating under the same network. For example, local IoMT includes home health monitoring, hospital patient monitoring, and care homes. Remote monitoring IoMT consists of systems and devices that are not within the same network. Examples of remote IoMT can be seen in public health monitoring, remote patient monitoring, and remote healthcare consulting through a General Practitioner.

1.3. Problem Statement, Research Aim, and Objectives

An IoT or any IoMT applications and systems need to ensure the safety and security of the devices, network, and data, especially when dealing with sensitive health and care data. As stated by [6], IoMT devices must incorporate confidentiality, integrity, and authentication within their designs to ensure the privacy of the user data and the accuracy of the data. As the IoMT refers to medical devices, the impact of a security incident could lead to permanent health consequences for patients and loss of life. This is a significant risk that requires great care. It has been generally neglected previously due to the difficulties in achieving a perfectly balanced state of security and system performance requirements. IoT devices are heavily resource-constrained, meaning significant challenges occur when incorporating security into these devices. So, computation and memory constraints are two components that may affect the level of security that can be incorporated into these devices because security features are resource-demanding in nature. So, there is a clear research gap regarding protecting the IoMT system when all the essential security features needed in protecting the data, devices, and network are taken into account, especially when the devices are a resource constraint. Medium Access Control (MAC) spoofing attacks are common when the network does not filter the MAC addresses and port security is not taken into account at the data link layer of switches. A framework for detecting the MAC and IP (Internet Protocol address) using network characteristics is provided in [7], and there are various methods adopted in detecting MAC spoofing attacks including using the signal strength of the attacker's device [8], and channel state information [9]. MAC spoofing can be prevented through port security at the data link layer, as highlighted in [10,11]. However, it is not appropriate to assume that port security is already enabled in every network, so developing a solution to avoid data leakage in the event of a MAC spoofing attack is one of the objectives of this research.

DoS and DDoS attacks are some of the most common cyber-attacks to take down network services. A detailed analysis of such DoS and DDoS attacks is given in [12]. An attack like DoS or DDoS can be detected using different methods including machine learning techniques [13] and hidden Markov models [14]. Such attacks in an IoT network can be prevented by using different methods including Blockchain technology, as described in [15,16], but they are resource-demanding solutions in nature. So, it is important to have a solution that is not resource-demanding in the process of avoiding DoS or DDoS attacks, which is one of the objectives of this paper. Moreover, when a security solution is developed, the system should not consider and concentrate only on a few security aspects while omitting other security features, leading to data disclosure to unauthorised users. So, to tackle these issues, security and privacy safeguarding mechanisms should be addressed from a holistic perspective. The proposed model will aim to ensure that the sensitive data of patients are collected securely by the sensors and confidentially transmitted to the server by maintaining data integrity, and that the data stored at the server are safeguarded from any form of unauthorised access. Thus, this paper is curated to aid secure-by-design solutions for smart hospital monitoring or remote home-based monitoring.

A security solution is not something that should be incorporated at the end or after the system development process, but rather it should be incorporated from the start of the design of the system and throughout the developmental process to safeguard the system as a whole and so that all the vulnerable points are mended as the system development progresses and it is this approach that is taken for this paper. The unique contributions of this paper are as follows: First, the approach of securing the data and the IoMT system by design and the process by which the IoMT system authenticates, authorises, controls access, dynamically manages the keys, and maintains data confidentiality, integrity, and availability. Second, an in-depth performance comparative study of secure integration of the interaction and engagement of the IoMT client with the user, IoMT server, and web server is performed. Third, the self-healing process during network failure and data recovery is presented. Fourth, different methods of alerting (email, display, sound, etc.) for health and well-being events are explored, as well as ways of collecting diverse sensory information (movement, temp, humidity, light, air quality, proximity, pressure, multimedia, etc.) to learn about the quality and well-being of the users and data visualisation. Lastly, exploring the best encryption and data signing processes to support real-time communication is also one of the key highlights of this paper. The proposed system of this paper ensures that Medium Access Control (MAC) spoofing will not impact the confidentiality and integrity of the data even if man-in-the-middle attacks are underway due to MAC spoofing because the sessions are encrypted. Moreover, the IoMT device client is authenticated through a unique ID (hash of user's registration data (Υ), MAC address (∂), and a 32-bit random number (μ)) to detect and identify the participating devices. MAC spoofing will not allow data tampering because of the digital signature, and non-repudiation attacks are prevented by signing the data using the sender's private key. Information disclosure is highly unlikely due to the high level of encryption and innovative dynamic key management policies. DoS and DDoS attacks are averted by monitoring the network and allowing only authorised and authenticated devices into the monitoring system.

The rest of this paper is structured as follows: Section 2 presents a state-of-the-art background discussion and detailed literature study on IoT-based health monitoring, IoMT, smart hospitals, data security, data privacy, etc. Section 3 discusses the research principles and methodologies adopted in this research work. Section 4 proposes a secure-by-design IoMT framework, with technical details. Section 5 provides the results and discussion, while Section 6 concludes the paper with future directions.

2. Background and Literature Study

The following section explores the transformative shift brought by IoMT applications in healthcare. In addition, an extensive relevant literature study is conducted on data security, data privacy, and security threats in IoMT applications in the following sub-sections.

2.1. IoMT Transforming Healthcare

The vulnerabilities of the National Health Service (NHS) were illuminated during the chaos of the COVID-19 pandemic. The chaos revealed a system drastically underprepared to deal with surges of in-patient visits. The IoMT could and has reshaped the healthcare industry, bringing it forward into a new age of patient medical care. As stated in [17,18], the IoMT has been a significant contributor to developing and enhancing the infrastructure of hospitals and the way that medical professionals can provide care for patients. The IoMT allows for continuous real-time monitoring and tracking of patients; due to its lightweight form, this can be achieved with minimal discomfort to patients. In addition, applications of the IoMT with wireless communication allow the patient to freely move around and maintain mobility. Advancements in remote patient monitoring also make it possible for detailed and accurate data on patients to be gathered while they are in their own homes. The IoMT has the added benefits of allowing for decreased hospital bills due to its affordability, scalability, and ease of adoption, leading to overall cost savings.

2.2. Smart Healthcare Facilities

The recent turmoil of the COVID-19 pandemic has pushed society towards using smart hospitals as a solution to the NHS's vulnerabilities. It is important to highlight that this transformation is not to replace individuals such as healthcare professionals, but rather to improve their abilities and resources. This, in turn, will enhance patient care, and smart hospitals use these integrated technologies to conduct real-time monitoring and automated processes to create an interconnected healthcare ecosystem that enhances patient care, improves operational efficiency, and promotes innovation in the healthcare industries [19,20]. The ratio of nurses to patients within hospital settings is lower than that in any other healthcare setting, and such observations have been reported and studied in different healthcare settings [21–26] across different countries. Hence, there is a real need for a solution to relieve the strain these healthcare professionals experience. Real-time monitoring provides an opportunity for a solution to this strain. Real-time data monitoring enables us to translate factors from the environment, resources, and patients into usable data that can be used and acted upon. Indeed, advanced wearable health monitoring is transforming remote population health monitoring and changing the dynamics of the methods used for monitoring health in society [27] and for communication in hospital management using IoMT [28]. It is also important to make such medical devices portable and monitorable, and such a system is highlighted in [29]. Moreover, during the monitoring process, understanding the activity context recognition during ambient sensing is important [30]. So, developing smart innovative solutions for such a system is necessary to make it effective and efficient. Some incorporate AI into such systems to infuse intelligence into the medical device system [31]. However, there are many challenges in developing and designing such solutions; among these, one of the key challenges that need to be addressed to make it acceptable is the security and privacy issue [32,33]. So, an analysis of medical devices and software to detect and identify security vulnerabilities is necessary to make such systems safe [34].

2.3. Necessity of Data Security and Privacy

Reaping the great benefits of these smart systems can provide a plethora of new challenges. There is a necessity for the production and collection of masses of data within smart systems, and these data must be held with the highest levels of privacy and security. This is essential to maintain the integrity, reliability, and confidentiality of overly sensitive patient data, health records, and healthcare providers' reputations, as well as trust. Data mismanagement may lead to disciplinary measures against healthcare providers who fail to adhere to mandatory laws and regulations. Examples of these laws that are mandatory to follow when processing patient data include the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States of America and the General Data Protection Regulation 2018 (GDPR) in the European Union. Non-compliance with such laws can result in disciplinary action, fines, lawsuits, and loss of accreditation. Moreover, the accuracy and reliability of data are essential to safeguard the integrity of clinical decision-making and research findings, ensuring they remain unbiased and uninfluenced.

In summary, healthcare data must be securely and confidentially managed, safeguarding both patients from potential harm and healthcare providers from legal liabilities. On the other hand, as straightforward as this may seem, many providers cut corners when following these regulations and laws. A review of IBM's *Threat Intelligence* report [35] uncovers alarming statistics for security within healthcare. It is one of the top ten sectors affected by cyber threats and exploits. It is also highlighted that backdoor attacks were detected in 27% of the cases, followed by web shells in 18%. Adware, Business Email Compromise (BEC), cryptocurrency miners, loaders, reconnaissance and scanning tools, and remote access tools accounted for 9% each. Among the observed impacts, reconnaissance was the most prevalent, constituting 50% of the cases. Additionally, data theft and digital currency mining were identified in 25% of cases each. There are other forms of cyber-attacks, e.g., predictive jamming attacks in IoT infrastructure like LoRaWAN [36] and hacking into a pacemaker [37]. For a better understanding of what kind of cyber-attacks happened within the healthcare industry, some news and literature are shown in Table 1, outlining the attacks, the nature of the attacks that occurred (in no order), and possible mitigation techniques that need to be incorporated to safeguard the system [38–47], while the nature of these cyber-attacks is listed in [48–57], followed by an elaboration of each attack in the following paragraphs.

SQL Injection: A type of security vulnerability that allows an attacker to interfere with the queries an application makes to its database. Such vulnerability occurs when an attacker can insert or inject malicious SQL code into a query. This can lead to various harmful outcomes, such as unauthorised access to sensitive data, data modification, or even deletion of the entire database.

Zero-Day Exploits: A type of cyber-attack that targets a software vulnerability unknown to the software developer or the public. Because the developers are unaware of the vulnerability, there is no patch or fix available at the time of the attack, making it particularly dangerous and effective to the attacker.

Insider Threats: These refer to risks posed by individuals within an organisation who have access to critical systems and data. These threats can come from employees, contractors, business partners, or anyone else with inside knowledge and access to the organisation's operations. Insider Threats can be intentional, such as sabotage or data theft, or unintentional, such as accidental data breaches or policy violations.

Phishing: A type of cyber-attack in which attackers deceive individuals into providing sensitive information such as usernames, passwords, credit card numbers, or other personal details. This is typically achieved by masquerading as a trustworthy entity in electronic communications.

Table 1. Attacks most likely to target the healthcare industry and their mitigations.

Cyber Attack Name	Description	Mitigation	Impact Example
SQL Injection [48]	Malicious code injected via web application vulnerabilities to gain unauthorised access.	Use parameterised queries, input validation, and access controls to restrict unauthorised database access.	Community Health Systems in the US lost 4.5 million patient records in a 2014 SQL Injection attack [38].
Zero-Day Exploits [49]	Using undiscovered hardware or software flaws for unauthorised access.	Implement intrusion detection/prevention systems, monitor for unusual activity, and stay updated with security advisories.	Hacking Team's 2015 breach revealed several zero-day vulnerabilities in widely used software [39].
Insider Threats [50]	Staff or subcontractors with access to patient data might inadvertently cause harm or steal information.	Set access controls, monitor user behaviour, run background checks, and offer regular cybersecurity training to staff.	A former employee of a New York health system was indicted in 2015 for stealing information on over 12,000 patients and selling it on the dark web [40].
Phishing [51]	False emails trick users into revealing sensitive data.	Provide cybersecurity training, use email filters, and employ two-factor authentication to prevent phishing attacks.	Anthem, a US health insurer, lost 78.8 million patient details in a 2015 phishing attack [41].
Password Attacks [52]	Cracking passwords for unauthorised access; includes brute force or dictionary attacks.	Enforce strong password regulations, regular changes, and complexity requirements, and establish two-factor authentication.	During a credential-stuffing attack on Magellan Health in 2020, 365,000 patients' information was stolen [42].
Malware [53]	Dangerous software, like viruses, trojans, and ransomware, that can steal data or corrupt systems.	Implement anti-malware software, perform routine backups, and keep systems updated with security patches.	The NHS in the UK faced the WannaCry ransomware in 2017, demanding ransom for file decryption [43].
Supply Chain Attacks [54]	Infiltrating healthcare systems through third-party hardware or software providers.	Monitor third-party vendors, enforce strict contracts, and conduct routine risk assessments.	Cyber-attack on software developer SolarWinds compromised businesses, including healthcare providers, in 2020 [44].
Social Engineering [55]	Coercing individuals into disclosing private information or performing certain tasks.	Regular cybersecurity training, security awareness programmes, and implementing security controls like spam filters and two-factor authentication.	Save the Children suffered a BEC attack in 2018, costing them GBP 1 million due to a fraudulent money transfer [45].
Misconfiguration [56]	Misconfiguring medical equipment or systems makes them vulnerable to intrusions or data breaches.	Adopt automated configuration management systems, secure configuration practices, and conduct routine auditing/testing of system configurations.	In 2018, 500,000 patients' information was stolen due to a misconfigured ransomware attack demanding submission at HMC in the US [46].
DoS/DDoS [57]	Overwhelming healthcare systems with traffic causes breakdowns or inaccessibility.	Implement network segmentation, deploy DDoS mitigation services/hardware, and create a DDoS response strategy.	It impacts the care services, and it can happen anytime. It has a massive amount of service interruptions [47]. WannaCry ransomware in 2017 [43] has a service denial impact.

Password Attacks: Such attacks are conducted to gain unauthorised access to systems and data by cracking or bypassing passwords. These attacks exploit weak or compromised passwords to infiltrate accounts and networks, leading to potential data breaches, identity theft, and other malicious activities.

Malware: Any software that is intentionally designed and developed to cause damage to a computer, server, client, or computer network. It can take many forms, including viruses, worms, trojans, ransomware, spyware, adware, and more. It aims to steal data, disrupt operations, or gain unauthorised access to systems.

Supply Chain Attack: A type of cyber-attack where attackers target the less secure elements of a supply chain to infiltrate an organisation. It exploits vulnerabilities in the supply chain network, which can include software vendors, service providers, or other third-party partners. By compromising one of these entities, attackers can gain access to the primary target's systems and data.

Social Engineering Attack: This kind of attack aims to manipulate individuals into divulging confidential information, performing actions, or granting access to secure systems. These attacks exploit human psychology rather than technical vulnerabilities, making them particularly effective.

Misconfiguration Attack: This kind of attack exploits vulnerabilities arising from improperly configured systems, networks, systems, or applications. These misconfigurations can occur due to errors, oversights, or lack of security best practices during the setup or maintenance of systems.

DoS/DDoS Attack: A malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic. The goal is to make the service unavailable to legitimate users by consuming its resources or causing it to crash. It can also be a protocol-based (SYN flood or Ping flood) or application-based (http GET/POST floods) attack.

2.4. Enhancing Data Security and Confidentiality in Smart Healthcare Settings

Understanding the necessity of data security and privacy pushes us toward the need to enhance data security and confidentiality in smart healthcare settings. With this new generation of data collection methods, it also poses the question of who the owner of the data is. The work of [58] states that there is a "lack of agreement about who the final data owner should be and uncertainty about what ownership exactly entails" when it comes to medical data in healthcare. This underscores the necessity for the healthcare sector to advance towards higher levels of data security, which can be achieved by addressing this issue. One potential approach is to establish precise definitions and clarifications concerning data ownership. NHS users are composed of various groups of healthcare professionals, local authorities, academics, auditors, commissioners, patients, health startups, and pharmaceutical companies. So, it is critical to know who can access what information and at what level. The data should be secured in such a way that access from unauthorised individuals is prevented. The system should ensure data Confidentiality (keeping information secret), Integrity (maintaining accuracy of information), and Availability (ensuring access to information by authorised users) as highlighted in [59]. Enhanced levels of data confidentiality can be enforced, where symmetric and asymmetric encryption keys can be used to allow varying levels of data security [60]. Research conducted by [61] has highlighted that high data latency can significantly impair the availability of data, emphasising the critical need for efficient Public Key Infrastructure (PKI) implementations to mitigate this issue. Another example includes Identity and Access Management (IAM). Such a system can perform different functions including authentication, authorisation, verification, and storage provision [62]. Security features are critical and have a significant impact on customers' trust and adoption of such technology [63]. One of the concerns regarding the IoMT security system is the leakage of personal information leading to a critical risk to patient privacy, but the IoMT system must ensure data confidentiality and preserve user data privacy [64–66] and the system must ensure non-repudiation [67]. However, due to the device's constraints, it is very challenging to incorporate security features. So, the encryption mechanisms must support low-powered devices [68], and a performance analysis of security features is conducted in [69]. Moreover, storage and processing are challenging when dealing with big data, so cloud computing can be combined with IoMT applications to enhance the system's performance. Cloud services provide the essential scalability factor, make the system flexible, and provide the necessary processing power needed to analyse vast datasets generated by IoT devices. This seamless integration enables real-time monitoring and reporting, transforming raw data into meaningful insights readily accessible to end users.

3. Materials and Research Methods

In this paper, the following research design in Figure 1 is used to arrive at the proposed secure-by-design solution by starting with a literature study followed by exploring the existing security solutions; then, the research gaps are identified, and the research aim, and objective are developed. There are different types of requirements including functional requirements, security requirements, system requirements, tools needed, and ethical considerations to successfully execute the design, development, and testing of the IoMT system.

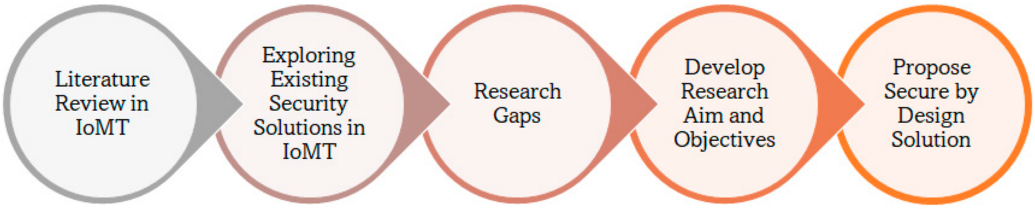

Literature Review in IoMT
Exploring Existing Security Solutions in IoMT
Research Gaps
Develop Research Aim and Objectives
Propose Secure by Design Solution

Figure 1. Research design.

3.1. Requirements

There are two main types of requirements, functional and non-functional, and there are different ways of defining and classifying them [70,71]. Functional requirements delineate the essential features and functionalities that the application must meet. On the other hand, non-functional requirements, while not directly enhancing system efficiency or security, aim to enhance user experiences.

3.1.1. Key Functional Requirements for the System

- Encrypted communication between devices and servers (IoMT and web server).
- Information integrity checking implementation for message verification.
- Information availability, authentication of users and devices, and non-repudiation functionality incorporation.
- Salting of the stored hashes to add the next level of security.
- Secure storage of data.
- Self-healing and no data loss during a network failure.

3.1.2. Other Non-Functional Requirements for the System

- Data visualisation for ease of data interpretation.
- Use of visual or auditable engagement like LEDs and buzzer sounds to be inclusive in the interaction and engagement.
- User's participation during the securing process.

The proposed system should allow local alerting to connect better with the response care team and local monitoring for observation and medical support. It should also support remote monitoring and remote alerting, as shown in Figure 2, to ensure ease of adoption and address the scalability and viability challenges in monitoring population health with an e-health monitoring system.

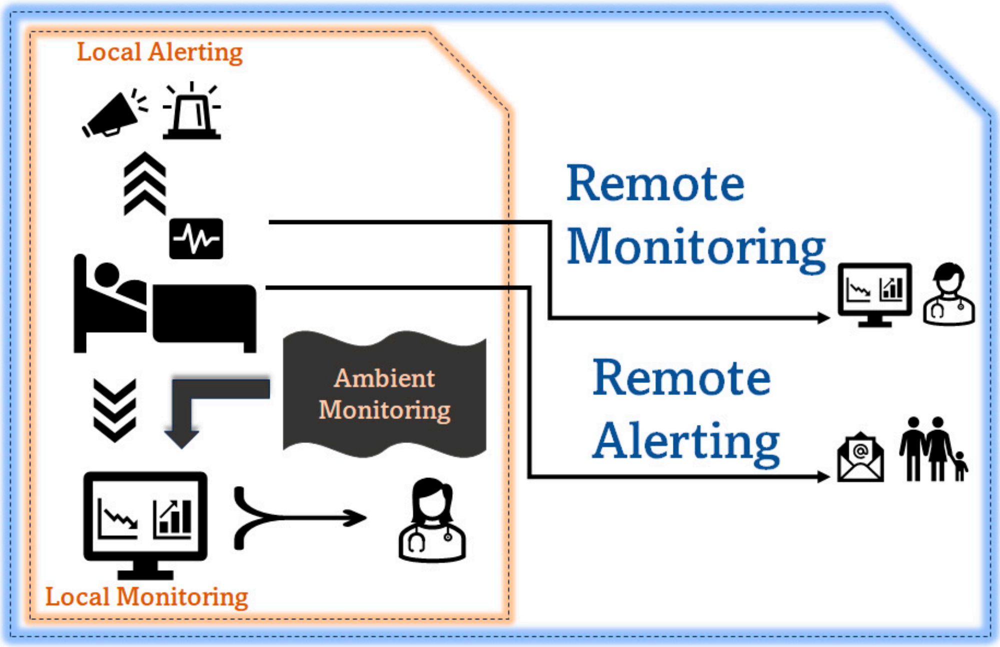


Figure 2. Use case diagram.

3.2. Security Constraints and Requirements

Incorporating security measures into resource-constrained devices poses significant challenges since the security mechanisms are influenced by computational limitations, memory constraints, and network restrictions. The authors of [69] also suggest that the IoT grapples with processing, storage, and network constraints. While solutions like the cloud could potentially address these constraints, they introduce additional security and privacy concerns since the majority of the storage or computation is carried out with third-party service providers. While balancing the above constraints, it is critical to maintain a balance between the minimum necessary security requirements, performance, and device constraints. It is critical to maintain the following key aspects in the process of developing secure IoMT infrastructure.

Data Confidentiality: Ensure all patient data are protected to prevent privacy violations or exposure to unauthorised third parties.
Integrity: Ensure that patient medical data are tamper-proof during the communication from the IoMT device to the server.
Authentication, Authorisation, and Access Control: Ensure that only authorised devices and users can join the network or begin communication to and from the server while participation is authorised and access to information is controlled.
Freshness: Ensure that real-time communication is achieved.
Non-Repudiation: Ensure data signing to validate where the data are originating from to ensure non-repudiation in the process of an identity attack.
Isolated Network: The system should be allowed to withstand network failure and be able to conduct self-healing in the process of data recovery when the network fails.

3.3. System Requirements

This paper developed an IoMT device by integrating raw sensors with a Raspberry Pi-based hardware computing system for data pre-processing. The IoMT system should be securely connected with the IoMT server, and the web server should interact with the IoMT server for data visualisation, user and IoMT device authorisation, and authentication. The Raspberry Pi 4 was used due to its low cost, high performance, and small and lightweight nature. The Raspberry Pi is equipped with Sense HAT and GrovePi+ sensors. The IoMT device, IoMT server, and web server are all executed in a Unix-based OS (Raspbian and

Ubuntu). The proposed system attempts to align system requirements with a robust acceptable solution mapped in Figure 3, where the device limitations and system performance should be taken into consideration when security mechanisms are incorporated to make the system ideally functional without compromising the security level. This is because resource-constraint-sensing systems will not be able to tolerate resource-demanding security solutions, e.g., it will be extremely challenging for low-powered sensing devices to incorporate resource-hungry security systems like Blockchain technology even if such a security solution is of high demand due to the high level of security features it provides [72].

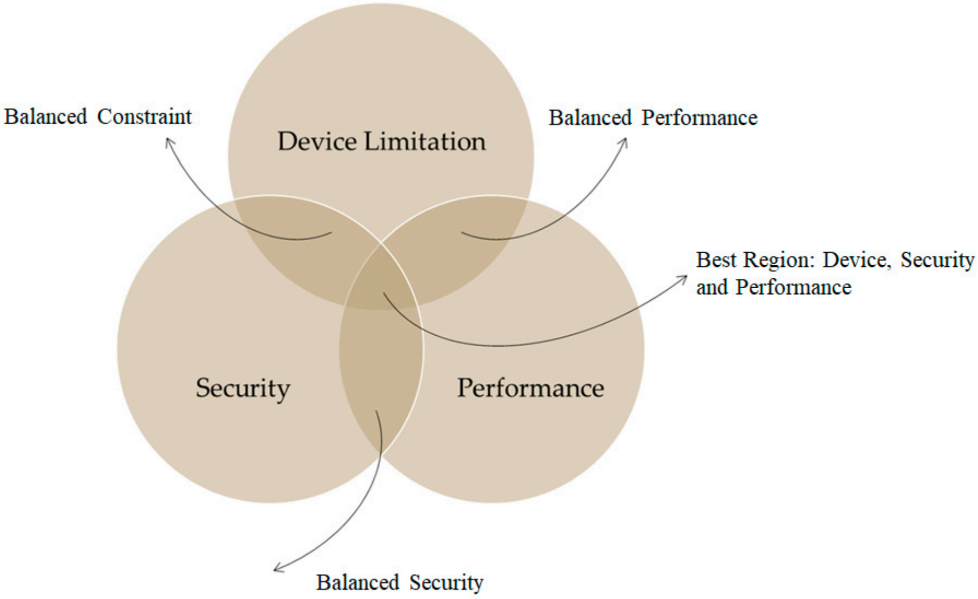


Figure 3. Proposed balanced system requirement over device limitation, security and performance.

3.4. Other Tools

Python 3 programming language was used for the client–server design and development, and XML, PHP, and JavaScript were used for web server development.

3.5. Testing Strategy

The data collection process is invoked when there is a change in the data read by the IoMT sensors to avoid sending the same data and reduce bandwidth overload. Throughout the testing, the network infrastructure remained constant, undergoing no changes that could influence the results. Key sizes for AES were 128, 192, and 256 bits, compared to RSA with key sizes of 1024, 2048, 4096, 7936, and 8192 bits, and for message integrity and digital signature, SHA 256 was used. During the testing, the room windows and doors were opened occasionally to test the air quality and blow on the heat and humidity sensing sensors to observe changes in temperature and humidity readings. Also, the IoMT device was moved, and the device was approached to test the functions of the alerting and evidence-collection aspects.

4. Proposed System and Architecture

This paper proposes a novel secure and lightweight privacy-safeguarding IoMT system, known as Secure-by-Design Real-Time IoMT Architecture for e-Health Population Monitoring (RTPM). This kind of system is best fit for monitoring well-being in two-fold, i.e., local monitoring (care home, hospital, etc.) and remote monitoring, as shown in Figure 3. The proposed IoMT device can collect diverse sensory information (movement, temperature, humidity, light, pressure, air quality, picture, or video) and display messages with LCDs, buzzers, and LEDs. The proposed RTPM is a secure-by-design solution that protects the data source (IoMT device), securely authenticates every participating IoMT device, safeguards data transmission channel from unauthorised access, ensures non-repudiation, protects data from MAC spoofing, conducts secure key management and authorises every user participating in the system to support auditing and accounting. Thus, the proposed system addresses all the key security issues about data confidentiality, data integrity, and data availability. The proposed system has the following key security and network features:

Data confidentiality: The communication and interaction between the IoMT client and the IoMT server (and the web server) are secured through a combination of RSA, AES, and SHA algorithms.

Data Integrity: All data generated by the IoMT client are signed, and the integrity of the data is preserved using SHA 256.

Authorisation, Authentication, and Access Control: User registration is conducted via the web server securely, and authorisation is needed to receive unique IDs for device authentication and for controlling access.

System Recovery and Self-Healing Network: If the client is disconnected, the last data block sent is remembered, and the data from the last point of failure continue to be sent automatically when the application is restarted.

Privacy-based Alerting Methods: The system can securely alert the user's selected individual using registered emails, e.g., doctor, carer, friends, or family (via email), when the condition of a monitoring outcome is not normal (e.g., when their body temperature is too high, or when the air quality of the room is bad).

System Monitoring and Evidence Collection: The system logs every exception, error, and abnormal event, e.g., lifting the IoMT device, coming close to the monitoring system, etc., to monitor physical intrusion.

Data Visualisation: The IoMT server is integrated with a web server, and the data are visualised for easy access. All the registered IoMT devices can be monitored from anywhere and at any time.

In addition, this paper conducts an in-depth performance-comparative study of the secure integration of the interaction and engagement of the IoMT client with the user, IoMT server, and the web server. This study enlightens the research community on what key sizes are appropriate for building a secure IoMT system, how to securely register users and devices, and what kind of data can be securely transmitted in real time.

4.1. RTPM Monitoring Architecture

The system is designed to be able to securely monitor health-related data, e.g., temperature and the sweating level of a patient, as well as the ambient space for well-being monitoring (movement, light, pressure, magnetic flux, air quality, etc.). The system also monitors and alerts surrounding people with messages via LCDs, buzzers, and LEDs to make them aware of the monitoring events. If the system is disturbed, then alert functions are activated; otherwise, the system continues to measure and update the server and relevant stakeholders (doctors, nurses, carer, friends, and family) depending on the condition of the patients and the environment in which the patient is monitored, as shown in Figure 4. The user needs to hold the temperature and moisture/humidity sensor for data collection, and the rest of the data of the environment and the patient's well-being are continuously monitored at the same time. If the data do not change, then the sensory information is not transmitted to the server to reduce system overhead; however, if the data remain constant for over 5 min, then the data are pushed to the server to ensure the system's liveness. The system can detect if there is movement, if the device is disturbed, if the brightness of the room is changed, or if the air quality and pressure of the room change. Such a system is perfect for monitoring population health in general and is perfect for a situation like the COVID-19 pandemic. The system can be deployed locally in a hospital, remote care, or home environment. The architecture ensures that the IoMT device is securely registered and authorised, the data are transmitted securely (confidentiality and integrity maintained), the data source is identified, only authorised users access or receive the data, security keys are safely exchanged or delivered, fresh session keys generated for every connection request, and the storage is securely locked.

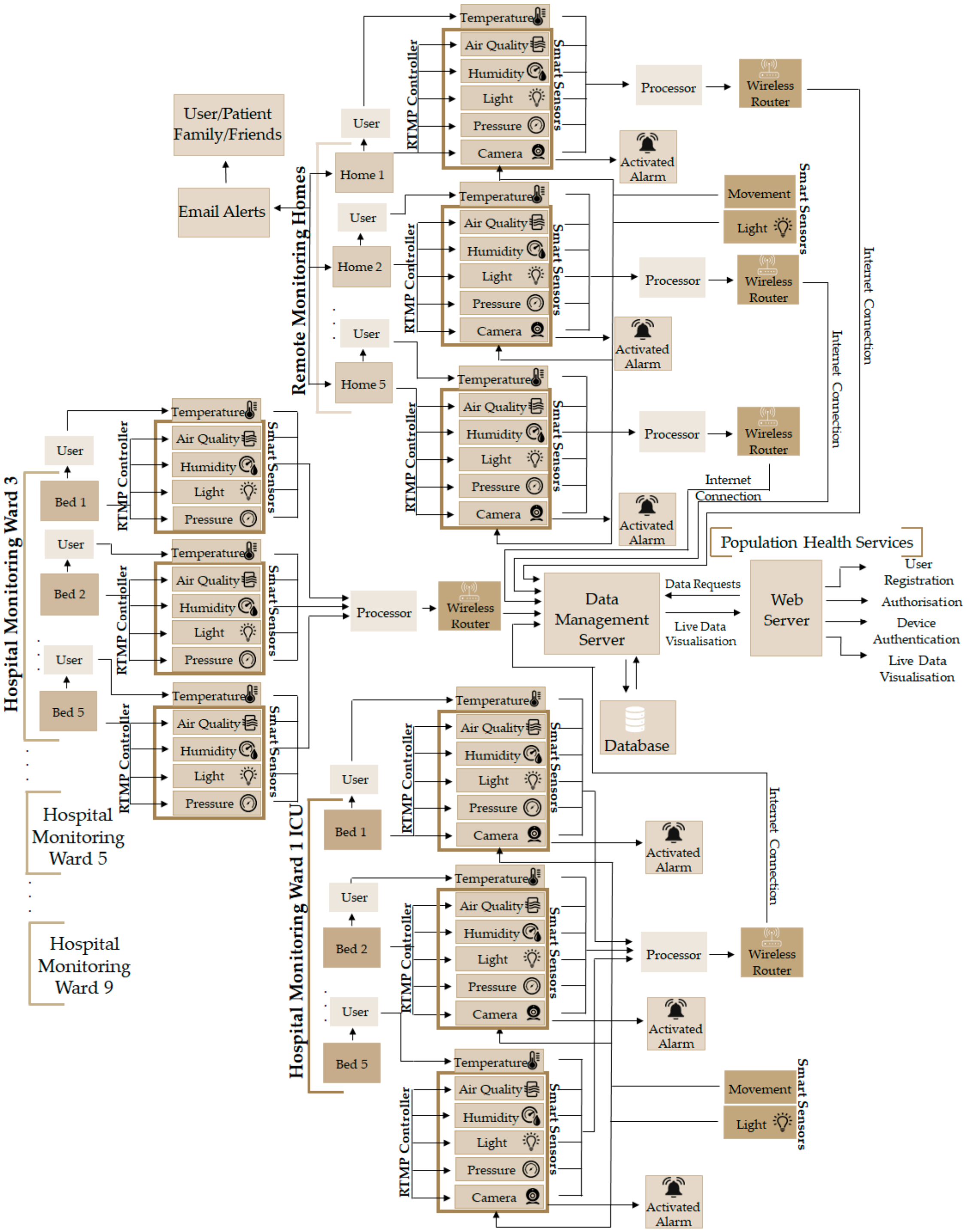


Figure 4. Proposed IoMT monitoring architecture.

4.2. RTPM Controller at the Client

The IoMT device is activated with a unique ID that is supplied during the registration process of the user, and along with the NHS number, the device is uniquely identified by the server. The monitoring events are grouped into four strands, namely device protection, alerting or alarming, space quality, and health condition aspects. Due to the lack of compatible sensors to integrate with the designed system, some health-sensing systems like those for heart rate, ECG, and oxygen level could not be integrated. The system continually monitors the user and their environment, as shown in Figure 5, and it records every event and piece of evidence including errors to monitor issues and identify reasons for failures of the system. The controller monitors the events and activities of all four activity strands and alerts the concerned and relevant stakeholders including the people around the room if they come too close, move the device, or try to steal it. In such an event, evidence is collected in the form of movement detection, snapshots of the environment are captured with the camera, and the evidence is securely transmitted to the server for investigation and service quality monitoring (to find out who touched the device, when and how often, etc.).

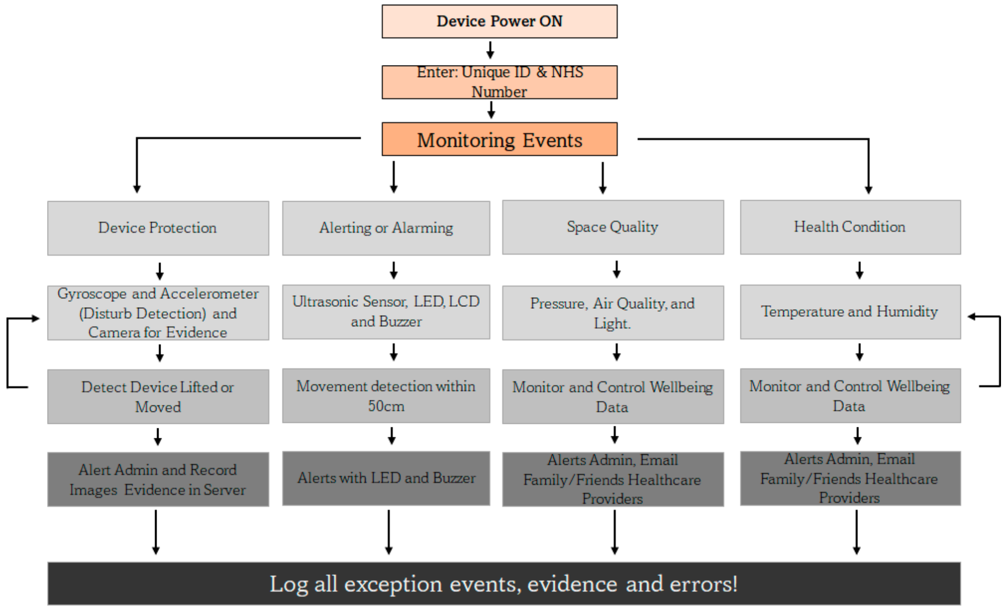

Device Power ON
Enter: Unique ID & NHS Number
Monitoring Events
Device Protection
Alerting or Alarming
Space Quality
Health Condition
Gyroscope and Accelerometer (Disturb Detection) and Camera for Evidence
Ultrasonic Sensor, LED, LCD and Buzzer
Pressure, Air Quality, and Light.
Temperature and Humidity
Detect Device Lifted or Moved
Movement detection within 50cm
Monitor and Control Wellbeing Data
Monitor and Control Wellbeing Data
Alert Admin and Record Images Evidence in Server
Alerts with LED and Buzzer
Alerts Admin, Email Family/Friends Healthcare Providers
Alerts Admin, Email Family/Friends Healthcare Providers
Log all exception events, evidence and errors!

Figure 5. RTPM controller architecture of the client.

4.3. RTPM User, Device, and Key Management

The keys are managed as shown in Figure 6. The client IoMT devices are capable of generating keys. To build and retain confidence and trust among the users who adopt such monitoring technology, the end user's devices generate their public and private key pair, the public key is shared with the server, and the server does likewise. This does not mean the server cannot generate and distribute keys to the client. It means the user's trust level will be higher when it generates their key rather than a third party providing it. In this proposed system, every user must register on the web server to receive a unique ID for the IoMT identification and authentication process. Every successful validation of the user registration leads to the creation of three different unique hashed HEX digits using SHA 256, namely verified ID (Υ) = SHA256 (user registration information), unique client ID (∂) = SHA256 (MAC address), and random number (μ) = SHA256 (32 digits), and these data are used for the IoMT identification and authentication during the device connection to the server, as shown in Figure 6. The unique ID used during the device identification = SHA256 ($\Upsilon + \partial + \mu$), and since its raw data are within the server, it can validate the hash value and authenticate it. Thus, in the first step, user registration along with verification is conducted as shown in Figures 7 and 8, which elaborate on how the authorisation process is conducted to verify the authenticity of the user. Figure 9 shows the connection request made by the IoMT client to the IoMT server and how the signature validation is executed when exchanging the public keys. The IoMT server and the web server are hosted on the same machine. The public keys of the IoMT server and the IoMT devices are exchanged once the client's connection is established successfully, as shown in steps 2, 3 and 4 of Figure 6. The IoMT server is responsible for creating the session keys for secure data transmission from the IoMT clients. The session key is an AES key and is delivered to the IoMT clients by the IoMT server by securely signing to ensure that the originator's identity and data integrity (using SHA 256) are maintained, as shown in step 5. The data transmission from the IoMT clients for the session is conducted by using AES 256, which is provided by the IoMT server, and signing the data using SHA 256, as explained in step 6 of Figure 6 where the IoMT client's private keys = {RSA PrivK-1, RSA PrivK-2, . . ., RSA PrivK-N} and public keys = {RSA PubK-1, RSA PubK-2, . . ., RSA PubK-N}. The session key is represented by the AESSession Key, the IoMT server's private key is RSA PriK-S, and the public key is RSA PubK-S.

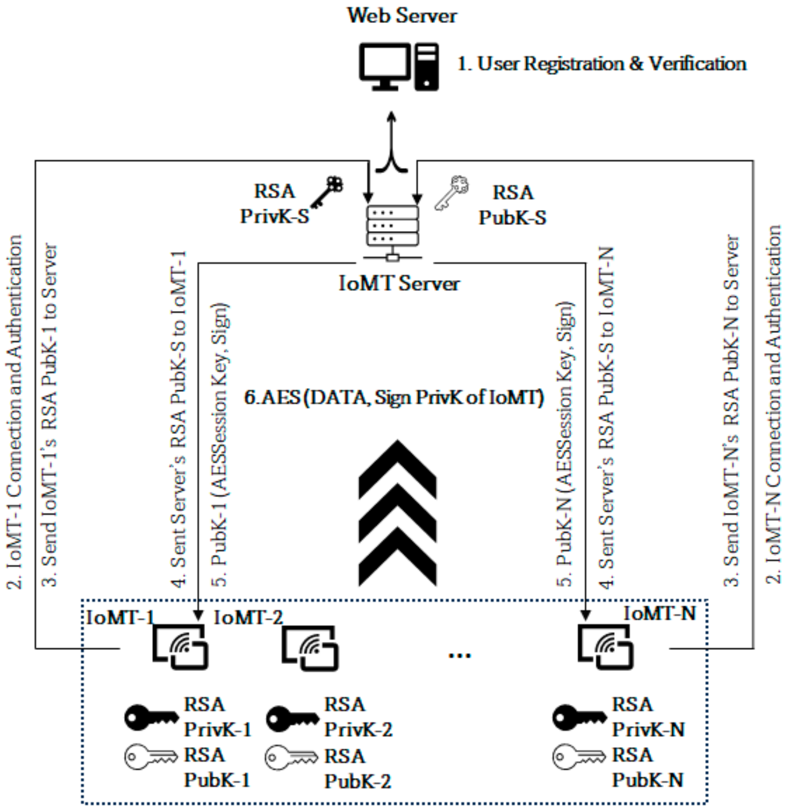
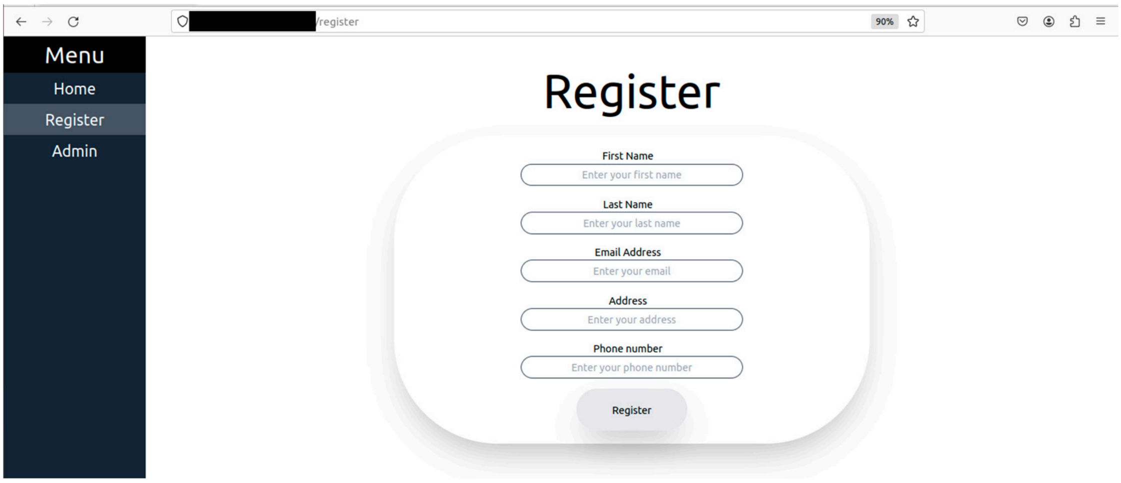

Web Server
1. User Registration & Verification
RSA PrivK-S
RSA PubK-S
IoMT Server
2. IoMT-1 Connection and Authentication
3. Send IoMT-1's RSA PubK-1 to Server
4. Sent Server's RSA PubK-S to IoMT-1
5. PubK-1 (AESSession Key, Sign)
6.AES (DATA, Sign PrivK of IoMT)
5. PubK-N (AESSession Key, Sign)
4. Sent Server's RSA PubK-S to IoMT-N
3. Send IoMT-N's RSA PubK-N to Server
2. IoMT-N Connection and Authentication
IoMT-1
IoMT-2
...
IoMT-N
RSA PrivK-1
RSA PubK-1
RSA PrivK-2
RSA PubK-2
RSA PrivK-N
RSA PubK-N

Figure 6. Model network diagram of key management.



Register

First Name
Enter your first name

Last Name
Enter your last name

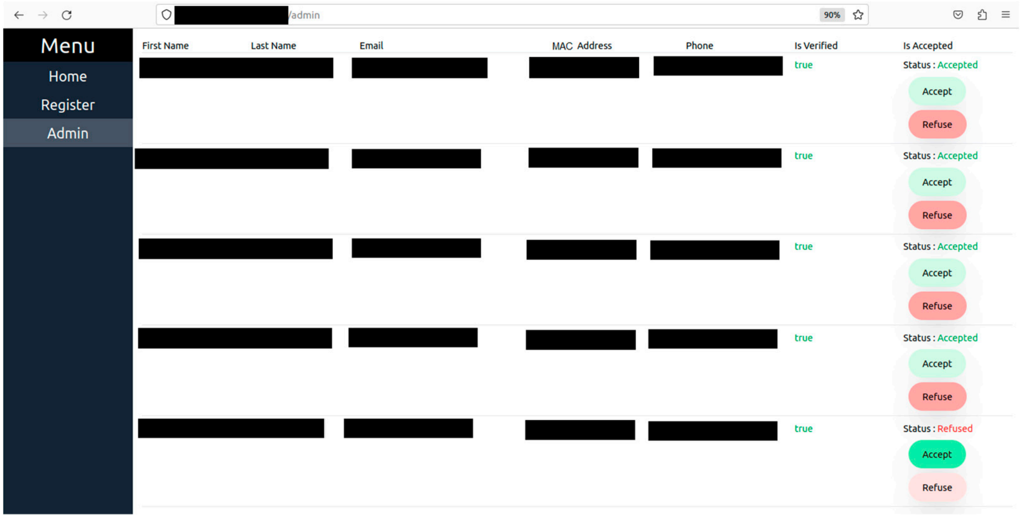
Email Address
Enter your email

Address
Enter your address

Phone number
Enter your phone number

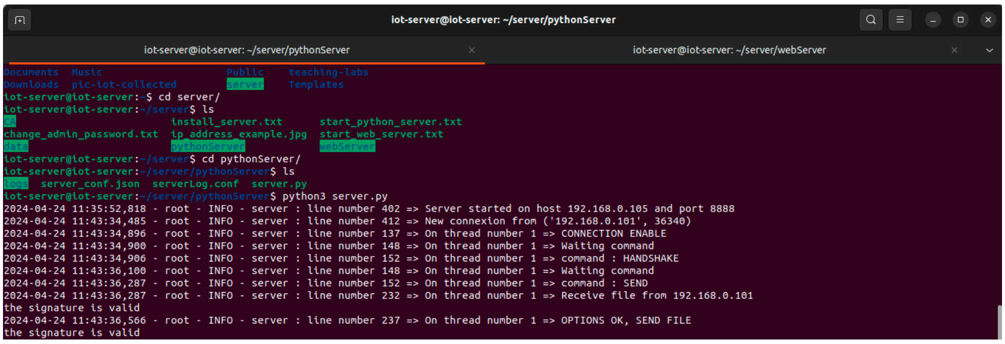
Register

Figure 7. User registration for monitoring.



First Name	Last Name	Email	MAC Address	Phone	Is Verified	Is Accepted
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	true	Status : Accepted Accept Refuse
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	true	Status : Accepted Accept Refuse
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	true	Status : Accepted Accept Refuse
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	true	Status : Accepted Accept Refuse
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	true	Status : Refused Accept Refuse

Figure 8. User authorisation process.


iot-server@iot-server: ~/server/pythonServer
iot-server@iot-server: ~/server/pythonServer
iot-server@iot-server: ~/server/webServer

```
Documents  Music                    Public    teaching-labs
Downloads  pic-iot-collected        server    Templates
iot-server@iot-server:~$ cd server/
iot-server@iot-server:~/server$ ls
CA                          install_server.txt      start_python_server.txt
change_admin_password.txt   ip_address_example.jpg  start_web_server.txt
data                        pythonServer            webServer
iot-server@iot-server:~/server$ cd pythonServer/
iot-server@iot-server:~/server/pythonServer$ ls
logs  server_conf.json  serverLog.conf  server.py
iot-server@iot-server:~/server/pythonServer$ python3 server.py
2024-04-24 11:35:52,818 - root - INFO - server : line number 402 => Server started on host 192.168.0.105 and port 8888
2024-04-24 11:43:34,485 - root - INFO - server : line number 412 => New connexion from ('192.168.0.101', 36340)
2024-04-24 11:43:34,896 - root - INFO - server : line number 137 => On thread number 1 => CONNECTION ENABLE
2024-04-24 11:43:34,900 - root - INFO - server : line number 148 => On thread number 1 => Waiting command
2024-04-24 11:43:34,906 - root - INFO - server : line number 152 => On thread number 1 => command : HANDSHAKE
2024-04-24 11:43:36,100 - root - INFO - server : line number 148 => On thread number 1 => Waiting command
2024-04-24 11:43:36,287 - root - INFO - server : line number 152 => On thread number 1 => command : SEND
2024-04-24 11:43:36,287 - root - INFO - server : line number 232 => On thread number 1 => Receive file from 192.168.0.101
the signature is valid
2024-04-24 11:43:36,566 - root - INFO - server : line number 237 => On thread number 1 => OPTIONS OK, SEND FILE
the signature is valid
```

Figure 9. Connection establishment, identification, and authentication.

5. Results and Discussion

The system is developed using the principle of security by design so that the security mechanisms and aspects are not added later, but incorporated during the system development process. As a result, the system interacts and engages securely between the IoMT client, the IoMT server, and the web server. The system communicates securely, the integrity of the data is preserved, there is strong authentication and access control, accounting and logging of every exception and error are conducted for incident response and recovery, client system recovery after network failure is provided, and a secure network design is incorporated to protect the system from DoS and DDoS attacks. The following is a discussion of the security features incorporated into the IoMT system.

(a) Data confidentiality: It is crucial to maintain data confidentiality since it deals with health and/or well-being-related data. The proposed system interacts and engages with the client node and the IoMT server using an AES session key, which is generated and provided by the server to the IoMT client. The session key is securely delivered using RSA public key cryptography, and the key is signed to guarantee the source of the generation and maintain the integrity of the information. The client and the server are both capable of generating keys. To maintain freshness and preserve security, the session keys are generated for every new connection and each session. Table 2 provides the security method's overhead in terms of time of execution, and these results are tested using the IoMT client (Raspberry Pi 4) with the following configuration: Broadcom BCM2711 SoC with a 1.8 GHz, 64-bit quad-core ARM Cortex-A72 processor with 4 GB RAM, and the IoMT server executing with 64-bit, Intel Core i7, CPU @2.6 GHz with 32 GB RAM. The system is tested with various key sizes (standard and above) to select the best key sizes for performing real-time communication. The results of Table 2 are average values of executing over 10 rounds for each key size. The key generation and the key file generation take exponentially more time as the key size increases. The AES key generation time, encryption time, and decryption time take only a few milliseconds irrespective of the key sizes (128 bits, 192 bits, or 256 bits), while the RSA takes a little less than a second only for key sizes below 2048 bits for key generation, but takes some seconds to minutes for key sizes of RSA 4096 and above. However, the RSA method of encryption takes from around 0.01 s to 0.07 s when the key size increases from RSA 1024 bits to RSA 8192 bits. On average, the decryption time takes more than the encryption time. To meet the real-time requirement of interaction between the client and the server, the best option is the use of the AES encryption method while the secure session key transfer is conducted by RSA. To meet real-time requirements, this paper uses RSA 2048, AES 256, and SHA 256.

Table 2. Security methods and performance.

Methods	Cryptographic Algorithm (Seconds)							
Security processes	AES 128	AES 192	AES 256	RSA 1024	RSA 2048	RSA 4096	RSA 7936	RSA 8192
Key generation (IoMT)	0.000522	0.000554	0.000631	0.283	0.865	8.912	119.947	178.202
Key generation (server)	0.0001	0.000139	0.00014	0.215	0.731	4.708	49.21	54.043
Key file generation (IoMT)	0.002196	0.002214	0.002631	0.328	0.911	9.102	120.005	178.809
Key file generation (server)	0.000219	0.000221	0.000221	0.33	0.788	4.811	49.43	54.102
Encryption	0.000261	0.000261	0.000261	0.0149	0.015	0.0238	0.0688	0.072
Decryption	0.000042	0.000042	0.000043	0.0095	0.0202	0.0522	0.2802	0.3152
Digital signature	-	-	-	0.0011	0.0408	0.1744	0.9283	1.0355
Digital signature verification	-	-	-	0.00048	0.000829	0.00126	0.00387	0.00409

(b) Data Integrity: All data generated by the IoMT client are signed, and the integrity of the data is preserved using SHA 256 along with the privacy of the sender to avoid any form of non-repudiation attack. Creating a digital signature of the IoMT data takes 0.0011 s to 1.03 s when the RSA 1024-bit key and RSA 8192-bit key are used, respectively. As expected, as the key size increases, the digital verification takes longer, but it is more linear and not exponential. Since this paper uses an RSA 2048-bit key, it takes 0.04 s for signing and 0.0008 s for the verification, which is ideal for real-time communication.

(c) Data Availability (Authorisation, Authentication, and Access Control): To ensure data availability and protect the system from any form of DoS or DDoS attack, the proposed system authorises every user through a registration process, and a unique code is generated using SHA 256 with the help of the user's registration data (Υ), MAC address (∂), and a 32-bit random number (μ) at the IoMT server, which is provided to enter into the IoMT client as a unique ID = SHA256 ($\Upsilon + \partial + \mu$) during the device authentication process along with the NHS number to help the server uniquely identify and authenticate the connecting IoMT devices. This ensures that every connection request is unique, and the system also removes any idle connection requests (including any half-open connections using a timeout technique) to guarantee service availability.

(d) System Recovery and Self-Healing Network: One of the biggest issues when data collection is carried out over a network is the fear of network failure. In a real-time monitoring system, network failure will lead to data loss, but health and well-being data are critical, so all data should be delivered. So, in this system, a self-healing network system is adopted to recover and avoid data lost in the process of network failure. If the client is disconnected, the last data block sent is remembered, and the data continue to be sent from the last point of failure automatically when the application is restarted. So, the interaction of the client with the server is seamlessly synced without any data duplication or data loss when the network fails. To achieve this goal, the client reading the sensory data shares the same database with the application that connects with the server, and all data acknowledged by the server are set to 1 to determine what has been delivered and what is yet to be delivered otherwise.

(e) Privacy-based Alerting, Monitoring, and Evidence Collection: The system can securely alert the user’s selected individual, e.g., friends or family (via email), when the condition of the monitoring outcome is not normal (e.g., when the body temperature is too high or when the air quality of the room is bad). This is to support and update the carers and loved ones on the well-being of the user. The IoMT device detects when someone approaches and when someone touches or moves the IoMT device with the help of proximity, accelerometer, and gyroscope sensors and alerts about the events with a message, a red LED, and a buzzer. This is to ensure that the system is not disturbed, stolen, damaged, or moved unnecessarily when the system is in operation. If the alert messages are ignored and the IoMT device is touched or moved, then visual evidence is captured by a camera, and the evidence is securely transferred to the server. However, these settings can be disabled when the monitoring is conducted remotely from home, but these functions can be enabled when it is deployed in public care areas like hospitals to track and trace events in and around the patient for their safety and security. Figure 10 shows a warning message, while Figure 11 shows the alert message that is triggered when someone comes too close to the device, and Figure 12 shows the activation of the camera when someone attempts to take or move the IoMT device. These systems are necessary to give alerts on disturbances to the surroundings and also connect with the concerned stakeholders of the user.

(f) Visualisation of the Collected Data: The health and well-being environmental data that are collected from IoMT sensors can be viewed by the stakeholders through the IoMT server and web server. The screenshots of the temperature reading and moisture level of the skin when holding the sensors were collected using temperature and humidity sensors, and the results are shown in Figure 13. The spikes in the results are the results of blowing warm air through the mouth, which guarantees proper working of the system. The readings are taken from a snapshot record from 11:51:33 (AM) to 12:58:17 (PM), and the readings are taken every 5 s and updated on the server only when there is a change in the reading value; however, the IoMT client pushes the last recorded data even if there is no change if the time lapse over 5 min to ensure that the connection is live.

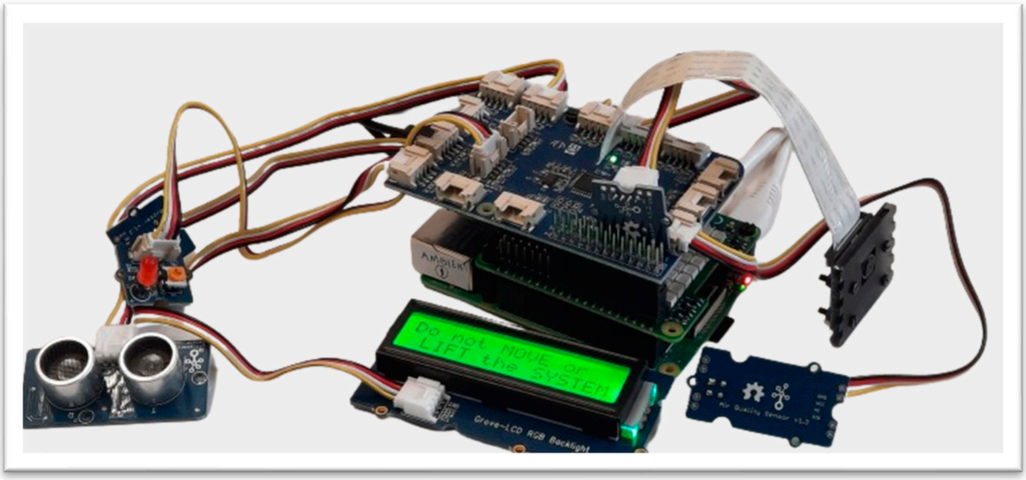


Figure 10. Warning message so that the device is not moved.

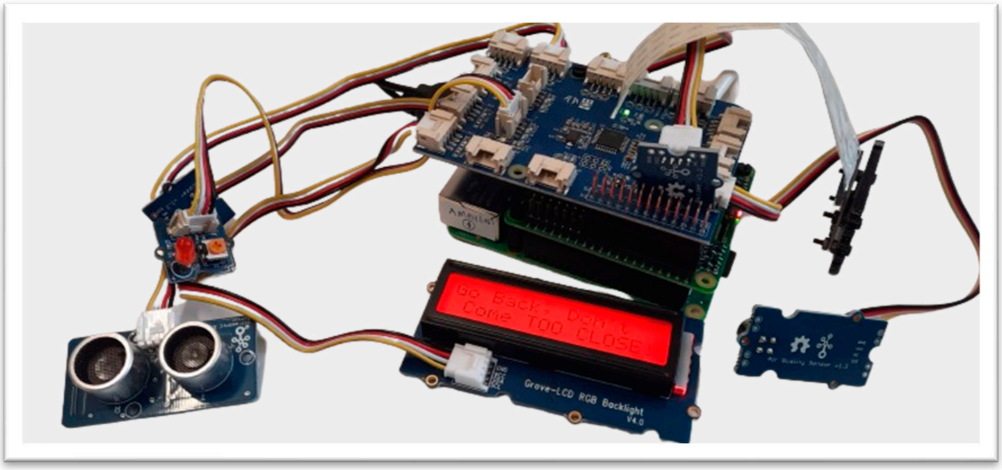


Figure 11. Warning when coming too close.

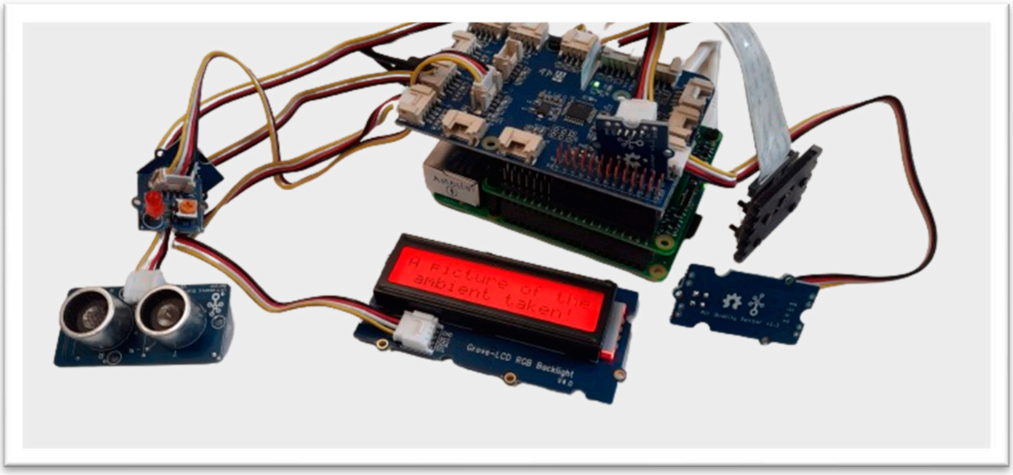


Figure 12. Capturing evidence if the system is moved.

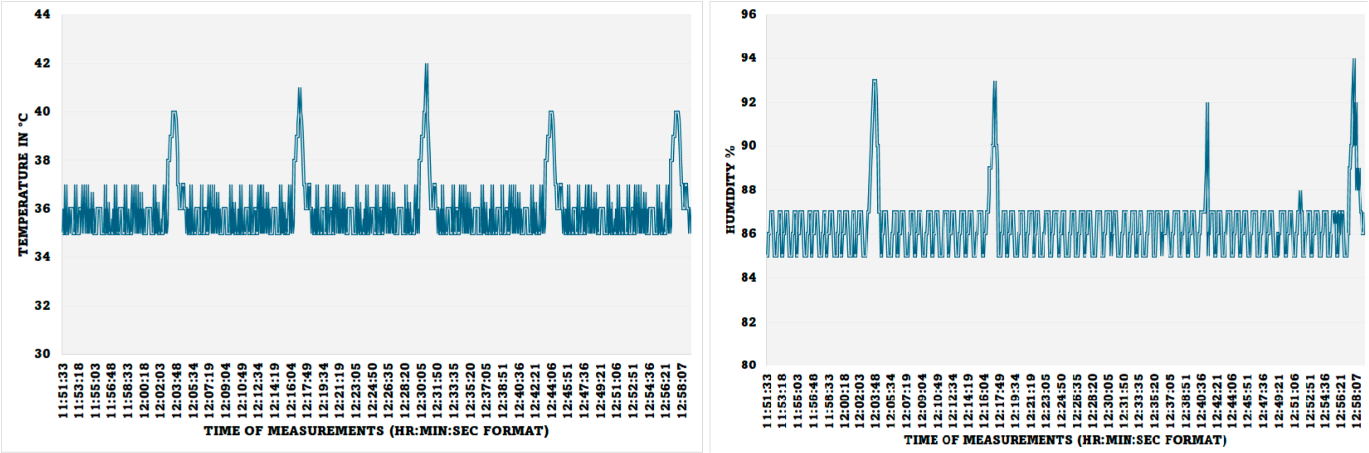


Figure 13. The body temperature and moisture level.

Figure 14 shows the measuring and monitoring of the air quality and the movement of people around the monitoring system. The positive incremental spikes from the normal reading in the air quality show that the air quality was decreased, which happened when five people sat around the IoMT sensor (more released CO_2), and the lower reading value of air quality occurring towards the end of the reading shows that the air quality was improved, which was triggered by the opened windows. The distance between the proximity sensor and the wall was measured as 110 cm, and the spikes are the result of introducing a human hand movement towards the proximity sensor at different times.

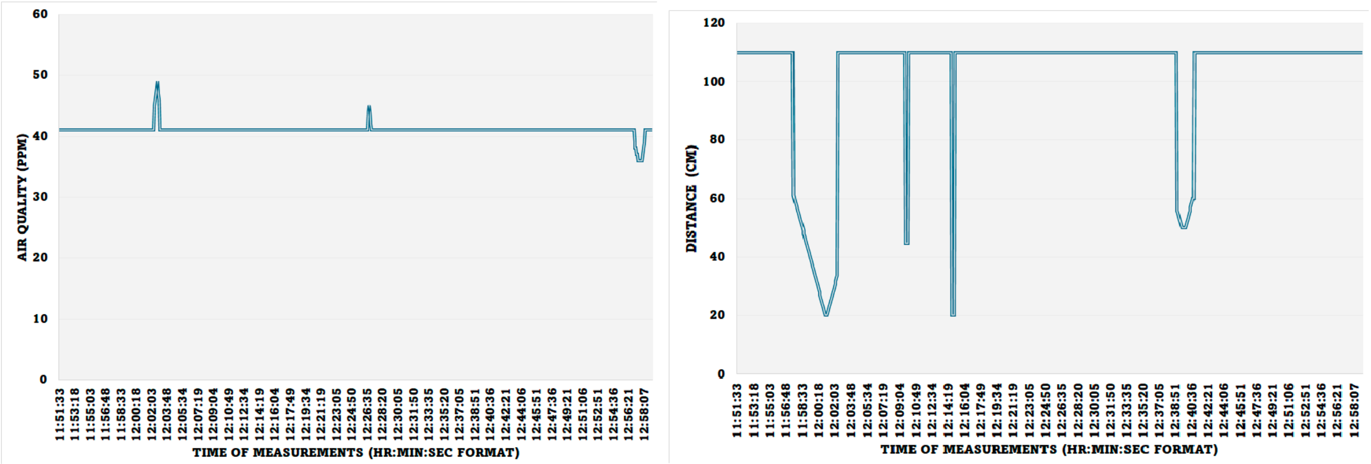


Figure 14. Air quality of the room and movement monitoring.

The light and noise levels were measured and recorded, as shown in Figure 15. The reading above 600 Lux is due to the introduction of more lighting around the sensor, and the reading going down is due to the closing of the window curtains. The normal lab sound record is 65 Db, the spikes are due to the noise of the servers running in the lab room, and the higher spikes are due to the introduction of a random human noise.

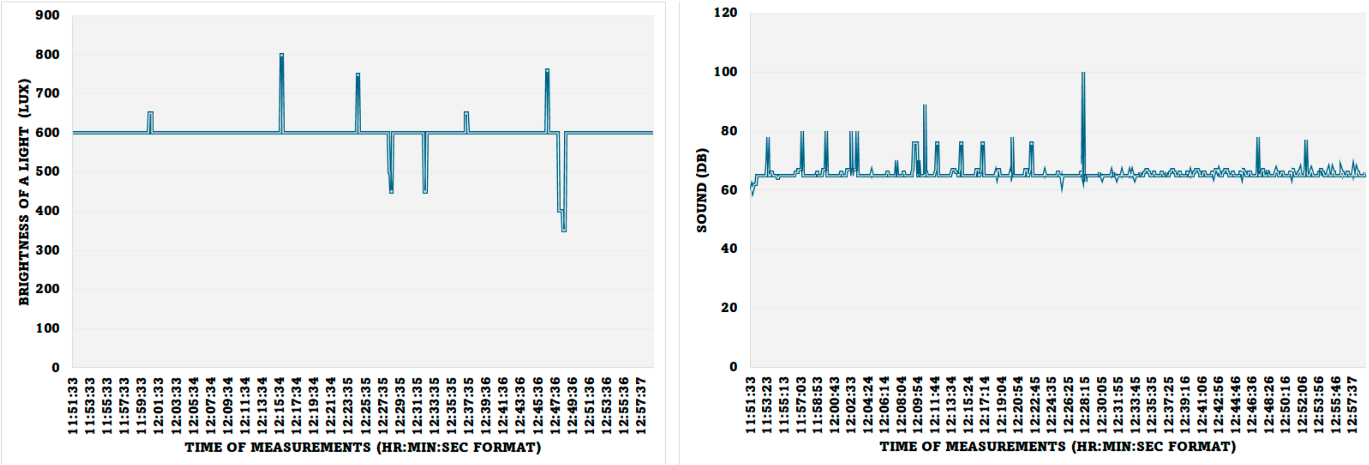


Figure 15. Lighting and noise monitoring.

6. Conclusions

This paper proposes a secure-by-design framework for monitoring health and well-being data for both local and remote monitoring. This system ensures that data confidentiality, data integrity, and data availability are maintained. It also ensures that only registered users are allowed to integrate the IoMT system into the health network, which helps in monitoring the connecting devices to protect the server from any form of DoS or DDoS attacks. To ensure real-time communication between the IoMT client and the server, it is necessary to use a secure key, but not a big key like RSA 4096 bits or above, because such key generation with a processing power of @1.8 GHz takes around 8–9 s; when it is an RSA 8192-bit key, it takes around 3 min on average, and when there is such a huge key size along with SHA 256, creating a digital signature and signing takes over 1 s. So, to meet real-time requirements, it is ideal to adopt the signing process using RSA 2048 for low computation power; however, due to the lightweight nature of the AES, any secure key sizes from a 128-bit key to an AES 256-bit key can be adopted for real-time communication. So, it is recommended to use RSA 2048, which is not too big for the signing process with SHA 256, to attain real-time communication in the process of avoiding a non-repudiation attack and to authenticate the sender. The level of security, system constraints, and performance of the system should be balanced, and no parameters should outweigh the others; otherwise, the system will not be usable. The developed system ensures that MAC spoofing does not compromise the data confidentiality and integrity by maintaining data encryption, signing the data, and authenticating using a unique ID to detect and identify the device. The proposed system does not allow data tampering during transit, repudiation attacks are not possible because of digital signature and signing using the sender's private key, information disclosure is not possible due to the high level of encryption and the adoption of dynamic key management policies, and DoS and DDoS attacks are averted by monitoring and allowing only authorised and authenticated devices into the monitoring system. The impact of such a system is that it is easy to deploy securely and easy to adopt, and the solution is scalable across the population for e-health monitoring locally or remotely from anywhere in the world as long as there is a network connection.

The developed system needs to be tested for its acceptance and adoption among potential users in hospitals and care homes to study the impact of such solutions, which will be carried out in future work. The system also needs to incorporate other aspects of secure-by-design features like the automatic detection of intrusion and threats, security controls, application failure recovery, patch management, etc. Other limitations of the proposed system are the lack of control over the access rights and limits over the data based on who is accessing them because the granularity of the data required by a doctor will be different from the nurse and so on. This aspect will be explored in the future. In terms of the hardware cost for the IoMT system development, it costs approximately GBP 120, mainly for using Raspberry Pi 4 with an HD camera and multiple sensors. The best thing about this prototype is that more sensors can be incorporated depending on the need with little or no modification to the system.

Author Contributions: J.M. (Jims Marchang), i.e., the corresponding author, and S.K. (Solan Keishing) designed and developed the framework and conducted the implementation, testing, and validation of the secure IoMT system. J.M. (Jade McDonald), K.Z. (Kavyan Zoughalian), R.M. (Raymond Mawanda), and B.S. (Ben Sanders) supported the work by conducting a critical literature study, supporting drafting the paper, and drawing the diagrams and figures. C.D.-B. (Corentin Delhon-Bugard) and N.B. (Nicolas Bouillet) supported J.M. (Jims Marchang) and S.K. in developing, implementing, and testing the IoMT client, IoMT server, and web server of the system. All authors have read and agreed to the published version of the manuscript.

Funding: The hardware and IoT/IoMT devices were funded by Sheffield Hallam University internally and we received no external funding for this project.

Data Availability Statement: The data were collected using the IoMT framework from a laboratory of the Computing Department of iSec CyberNet (https://shorturl.at/1IIUq (accessed on 4 July 2024)), and it is not appropriate to share the raw data. The source code can be shared with those who want to test it. Data are available on request due to restrictions (e.g., privacy and ethical reasons). The data presented in this study are available on request from the corresponding author.

Acknowledgments: We would like to thank Sheffield Hallam University for providing us with the necessary funds for buying IoMT devices, and for providing the cybersecurity lab resources for developing and hosting the web server, and for providing the network resources for testing in a real-world lab environment. We would also like to take the opportunity to thank Cindy Seram for proofreading the manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mohanta, B.; Das, P.; Patnaik, S. Healthcare 5.0: A Paradigm Shift in Digital Healthcare System Using Artificial Intelligence, IOT and 5G Communication. In Proceedings of the 2019 International Conference on Applied Machine Learning (ICAML), Bhubaneswar, India, 25–26 May 2019. [CrossRef]
2. Ashton, K. That "Internet of Things" Thing. *RFID J.* **2009**, *22*, 97–114. Available online: https://www.rfidjournal.com/that-internet-of-things-thing (accessed on 4 July 2024).
3. Scarpato, N.; Pieroni, A.; Nunzio, L.D.; Fallucchi, F. E-health-IoT Universe: A Review. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2017**, *7*, 2328. [CrossRef]
4. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [CrossRef]
5. Kakhi, K.; Alizadehsani, R.; Kabir, H.D.; Khosravi, A.; Nahavandi, S.; Acharya, U.R. The internet of medical things and artificial intelligence: Trends, challenges, and opportunities. *Biocybern. Biomed. Eng.* **2022**, *42*, 749–771. [CrossRef]
6. Sahi, M.A.; Abbas, H.; Saleem, K.; Yang, X.; Derhab, A.; Orgun, M.A.; Iqbal, W.; Rashid, I.; Yaseen, A. Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. *IEEE Access* **2018**, *6*, 464–478. [CrossRef]
7. Yu, J.; Kim, E.; Kim, H.; Huh, J. A framework for detecting MAC and IP spoofing attacks with network characteristics. In Proceedings of the 2016 International Conference on Software Security and Assurance (ICSSA), Saint Pölten, Austria, 24–25 August 2016; pp. 49–53.
8. Banakh, R.; Piskozub, A.; Opirskyy, I. Detection of MAC spoofing attacks in IEEE 802.11 networks using signal strength from attackers' devices. In Proceedings of the 1st International Conference on Computer Science, Engineering and Education Applications (ICCSEEA2018), Kiev, Ukraine, 18–20 January 2018; Springer: Cham, Switzerland, 2019; pp. 468–477.
9. Jiang, P.; Wu, H.; Xin, C. A channel state information based virtual MAC spoofing detector. *High Confid. Comput.* **2022**, *2*, 100067. [CrossRef]
10. Whalen, S. An Introduction to ARP Spoofing, Node99, Online Document. 2001, p. 563. Available online: https://priv.gg/e/arp_spoofing_intro.pdf (accessed on 4 July 2024).
11. Srinath, D.; Panimalar, S.; Simla, A.J.; Deepa, J. Detection and Prevention of ARP spoofing using Centralized Server. *Int. J. Comput. Appl.* **2015**, *113*, 26–30. [CrossRef]
12. Nayak, G.; Mishra, A.; Samal, U.; Mishra, B.K. Depth analysis on DoS & DDoS attacks. In *Wireless Communication Security*; Wiley: Hoboken, NJ, USA, 2022; pp. 159–182.
13. Al-Shareeda, M.A.; Manickam, S.; Ali, M. DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison. *Bull. Electr. Eng. Inform.* **2023**, *12*, 930–939. [CrossRef]
14. Balaji Bharatwaj, M.; Aditya Reddy, M.; Senthil Kumar, T.; Vajipayajula, S. Detection of DoS and DDoS attacks using hidden markov model. In Proceedings of the Inventive Communication and Computational Technologies conference (ICICCT 2021), Tamil Nadu, India, 8 May 2021; Springer: Singapore, 2021; pp. 979–992.
15. Ibrahim, R.F.; Abu Al-Haija, Q.; Ahmad, A. DDoS attack prevention for internet of thing devices using Ethereum blockchain technology. *Sensors* **2022**, *22*, 6806. [CrossRef]
16. Shah, Z.; Ullah, I.; Li, H.; Levula, A.; Khurshid, K. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. *Sensors* **2022**, *22*, 1094. [CrossRef]
17. Vishnu, S.; Ramson, S.J.; Jegan, R. Internet of medical things (IoMT)-An overview. In Proceedings of the 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 5–6 March 2020; pp. 101–104. [CrossRef]
18. Malasinghe, L.P.; Ramzan, N.; Dahal, K. Remote patient monitoring: A comprehensive study. *J. Ambient Intell. Humaniz. Comput.* **2017**, *10*, 57–76. [CrossRef]
19. Tabatabaei, S.M.; Kasrineh, M.R.; Sharifzadeh, N.; Soodejani, M.T. COVID-19: An Alarm to Move Faster towards "Smart Hospital". *Online J. Public Health Inform.* **2021**, *13*, 7. [CrossRef] [PubMed]
20. Michard, F.; Saugel, B.; Vallet, B. Rethinking the post-COVID-19 pandemic hospital: More ICU beds or smart monitoring on the wards? *Intensive Care Med.* **2020**, *46*, 1792–1793. [CrossRef] [PubMed]
21. Lake, E.T.; Shang, J.; Klaus, S.; Dunton, N.E. Patient falls: Association with hospital Magnet status and nursing unit staffing. *Res. Nurs. Health* **2010**, *33*, 413–425. [CrossRef] [PubMed]
22. Schubert, M.; Ausserhofer, D.; Desmedt, M.; Schwendimann, R.; Lesaffre, E.; Li, B.; De Geest, S. Levels and correlates of implicit rationing of nursing care in Swiss acute care hospitals—A cross sectional study. *Int. J. Nurs. Stud.* **2013**, *50*, 230–239. [CrossRef]
23. Neuraz, A.; Guérin, C.; Payet, C.; Polazzi, S.; Aubrun, F.; Dailler, F.; Lehot, J.J.; Piriou, V.; Neidecker, J.; Rimmelé, T.; et al. Patient mortality is associated with staff resources and workload in the ICU: A multicenter observational study. *Crit. Care Med.* **2015**, *43*, 1587–1594. [CrossRef] [PubMed]
24. McHugh, M.D.; Aiken, L.H.; Sloane, D.M.; Windsor, C.; Douglas, C.; Yates, P. Effects of nurse-to-patient ratio legislation on nurse staffing and patient mortality, readmissions, and length of stay: A prospective study in a panel of hospitals. *Lancet* **2021**, *397*, 1905–1913. [CrossRef]
25. Boyle, S.M.; Washington, R.; McCann, P.; Koul, S.; McLarney, B.; Gadegbeku, C.A. The nephrology nursing shortage: Insights from a pandemic. *Am. J. Kidney Dis.* **2022**, *79*, 113–116. [CrossRef] [PubMed]

26. Penturij-Kloks, M.M.; de Gans, S.T.; van Liempt, M.; de Vries, E.; Scheele, F.; Keijsers, C.J. Pandemic Lessons for Future Nursing Shortage: A Prospective Cohort Study of Nurses' Work Engagement before and during 16 Months of COVID-19. *J. Nurs. Manag.* **2023**, *2023*, 6576550. [CrossRef]
27. Tariq, M.U. Advanced wearable medical devices and their role in transformative remote health monitoring. In *Transformative Approaches to Patient Literacy and Healthcare Innovation*; IGI Global: Hershey, PA, USA, 2024; pp. 308–326.
28. Kim, B.; Kim, S.; Lee, M.; Chang, H.; Park, E.; Han, T. Application of an Internet of Medical Things (IoMT) to Communications in a Hospital Environment. *Appl. Sci.* **2020**, *12*, 12042. [CrossRef]
29. Siam, A.I.; El-Affendi, M.A.; Abou Elazm, A.; El-Banby, G.M.; El-Bahnasawy, N.A.; Abd El-Samie, F.E.; Abd El-Latif, A.A. Portable and real-time IoT-based healthcare monitoring system for daily medical applications. *IEEE Trans. Comput. Soc. Syst.* **2022**, *10*, 1629–1641. [CrossRef]
30. Ratnakar, A.; Enamamu, T.; Alfoudi, A.; Ikpehai, A.; Marchang, J.; Lee, G.M. Deep sensing: Inertial and ambient sensing for activity context recognition using deep convolutional neural networks. *Sensors* **2020**, *20*, 3803. [CrossRef] [PubMed]
31. Ratnakar, N.C.; Prajapati, B.R.; Prajapati, B.G.; Prajapati, J.B. Smart Innovative Medical Devices Based on Artificial Intelligence. In *Handbook on Augmenting Telehealth Services*; CRC Press: Boca Raton, FL, USA, 2024; pp. 150–172.
32. Osama, M.; Ateya, A.A.; Sayed, M.S.; Hammad, M.; Pławiak, P.; Abd El-Latif, A.A.; Elsayed, R.A. Internet of medical things and healthcare 4.0: Trends, requirements, challenges, and research directions. *Sensors* **2023**, *23*, 7435. [CrossRef] [PubMed]
33. Popoola, O.; Rodrigues, M.; Marchang, J.; Shenfield, A.; Ikpehia, A.; Popoola, J. A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, challenges and solutions. *Blockchain Res. Appl.* **2023**, *5*, 100178.
34. Mejía-Granda, C.M.; Fernández-Alemán, J.L.; Carrillo-de-Gea, J.M.; García-Berná, J.A. Security vulnerabilities in healthcare: An analysis of medical devices and software. *Med. Biol. Eng. Comput.* **2024**, *62*, 257–273. [CrossRef] [PubMed]
35. IBM Security X-Force Threat Intelligence Index. 2024. Available online: https://www.ibm.com/reports/threat-intelligence (accessed on 4 July 2024).
36. Ingham, M.; Marchang, J.; Bhowmik, D. IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN. *IET Inf. Secur.* **2020**, *14*, 368–379. [CrossRef]
37. Beavers, J.L.; Faulks, M.; Marchang, J. Hacking NHS pacemakers: A feasibility study. In Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019; pp. 206–212.
38. BBC News. Community Health Systems data hack hits 4.5 million. *BBC News*, 18 August 2014. Available online: https://www.bbc.co.uk/news/technology-28838661 (accessed on 10 May 2024).
39. Zetter, K. Hacking team's leak helped researchers hunt down a Zero-Day. *WIRED*, 13 January 2016. Available online: https://www.wired.com/2016/01/hacking-team-leak-helps-kaspersky-researchers-find-zero-day-exploit/ (accessed on 10 May 2024).
40. Staff, D.R. Former NY hospital employee admits to stealing colleagues' data. *Darkreading*. 11 December 2023. Available online: https://www.darkreading.com/cyberattacks-data-breaches/former-ny-hospital-employee-admits-to-stealing-colleagues-data (accessed on 10 May 2024).
41. US Department of Health and Human Services. Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History | Guidance Portal. 2020. Available online: https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach (accessed on 10 May 2024).
42. Davis, J. Magellan Health Data breach victim tally reaches 365K patients. *HealthITSecurity*, 19 October 2021. Available online: https://healthitsecurity.com/news/magellan-health-data-breach-victim-tally-reaches-365k-patients (accessed on 10 May 2024).
43. Mohurle, S.; Patil, M. A brief study of wannacry threat: Ransomware attack 2017. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 1938–1940.
44. Lazarovitz, L. Deconstructing the solarwinds breach. *Comput. Fraud. Secur.* **2021**, *2021*, 17–19. [CrossRef]
45. Muncaster, P. Save the Children hit by $1m BEC scam. *Infosecurity*, 28 April 2024. Available online: https://www.infosecurity-magazine.com/news/save-the-children-hit-by-1m-bec/ (accessed on 10 May 2024).
46. Wallace, F. Why data security has become a priority for healthcare professionals. *United States Cybersecurity Magazine*, 28 April 2024. Available online: https://www.uscybersecurity.net/healthcare/ (accessed on 10 May 2024).
47. U.S. Department of Health and Human Services. Health Sector Cybersecurity Coordination Center 2024. (HC3). ID#202405301200. Available online: www.HHS.GOV/HC3 (accessed on 10 May 2024).
48. Sadeghian, A.; Zamani, M.; Abdullah, S.M. A taxonomy of SQL injection attacks. In Proceedings of the 2013 International Conference on Informatics and Creative Multimedia, Kuala Lumpur, Malaysia, 4–6 September 2013; pp. 269–273.
49. Stellios, I.; Kotzanikolaou, P.; Psarakis, M. Advanced persistent threats and zero-day exploits in industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things*; Springer: Cham, Switzerland, 2019; pp. 47–68.
50. Liu, L.; De Vel, O.; Han, Q.L.; Zhang, J.; Xiang, Y. Detecting and preventing cyber insider threats: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1397–1417. [CrossRef]
51. Naaz, S. Detection of phishing in internet of things using machine learning approach. *Int. J. Digit. Crime Forensics* **2021**, *13*, 15. [CrossRef]
52. Alkhwaja, I.; Albugami, M.; Alkhwaja, A.; Alghamdi, M.; Abahussain, H.; Alfawaz, F.; Almurayh, A.; Min-Allah, N. Password cracking with brute force algorithm and dictionary attack using parallel programming. *Appl. Sci.* **2023**, *13*, 5979. [CrossRef]
53. Gaurav, A.; Gupta, B.B.; Panigrahi, P.K. A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterp. Inf. Syst.* **2023**, *17*, 2023764. [CrossRef]

54. Rao, V.V.; Marshal, R.; Gobinath, K. The IoT Supply Chain Attack Trends-Vulnerabilities and Preventive Measures. In Proceedings of the 2021 4th International Conference on Security and Privacy (ISEA-ISAP), Dhanbad, India, 27–30 October 2021; pp. 1–4.
55. Ghasemi, M.; Saadaat, M.; Ghollasi, O. Threats of social engineering attacks against security of Internet of Things (IoT). In Proceedings of the 1st International Conference on Fundamental Research in Electrical Engineering, Tehran, Iran, 26 July 2018; Springer: Singapore, 2019; pp. 957–968.
56. Srinivasa, S.; Pedersen, J.M.; Vasilomanolakis, E. Open for hire: Attack trends and misconfiguration pitfalls of IoT devices. In Proceedings of the 21st ACM Internet Measurement Conference 2021, Virtual, 2–4 November 2021; pp. 195–215.
57. Galeano-Brajones, J.; Carmona-Murillo, J.; Valenzuela-Valdés, J.F.; Luna-Valero, F. Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach. *Sensors* **2020**, *20*, 816. [CrossRef] [PubMed]
58. Martani, A.; Geneviève, L.D.; Elger, B.; Wangmo, T. It's not something you can take in your hands. Swiss experts' perspectives on health data ownership: An interview-based study. *BMJ Open* **2021**, *11*, e045717. [CrossRef]
59. Zhang, C.; Xia, J.; Yang, B.; Puyang, H.; Wang, W.; Chen, R.; Yan, F. Citadel: Protecting data privacy and model confidentiality for collaborative learning. In Proceedings of the ACM Symposium on Cloud Computing, Seattle, WA, USA, 1–4 November 2021; pp. 546–561.
60. Simmons, G.J. Symmetric and asymmetric encryption. *ACM Comput. Surv. CSUR* **1979**, *11*, 305–330. [CrossRef]
61. Qiu, T.; Chi, J.; Zhou, X.; Ning, Z.; Atiquzzaman, M.; Wu, D.O. Edge computing in industrial internet of things: Architecture, advances and challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2462–2488. [CrossRef]
62. Indu, I.; Anand, P.R.; Bhaskar, V. Identity and access management in cloud environment: Mechanisms and challenges. *Eng. Sci. Technol. Int. J.* **2018**, *21*, 574–588. [CrossRef]
63. AlHogail, A. Improving IoT technology adoption through improving consumer trust. *Technologies* **2018**, *6*, 64. [CrossRef]
64. Dzissah, D.A.; Lee, J.S.; Suzuki, H.; Nakamura, M.; Obi, T. Privacy enhanced healthcare information sharing system for home-based care environments. *Healthc. Inform. Res.* **2019**, *25*, 106. [CrossRef]
65. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput. Commun.* **2020**, *153*, 311–335. [CrossRef]
66. Elhoseny, M.; Ramírez-González, G.; Abu-Elnasr, O.M.; Shawkat, S.A.; Arunkumar, N.; Farouk, A. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access* **2018**, *6*, 20596–20608. [CrossRef]
67. Yeh, K.-H. BSNCare+: A Robust IoT-Oriented Healthcare System with Non-Repudiation Transactions. *Appl. Sci.* **2016**, *6*, 418. [CrossRef]
68. Tsai, K.-L.; Huang, Y.-L.; Leu, F.-Y.; You, I.; Huang, Y.-L.; Tsai, C.-H. AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments. *IEEE Access* **2018**, *6*, 45325–45334. [CrossRef]
69. Moosavi, S.R.; Nigussie, E.; Levorato, M.; Virtanen, S.; Isoaho, J. Performance Analysis of End-to-End Security Schemes in Healthcare IoT. *Procedia Comput. Sci.* **2018**, *130*, 432–439. [CrossRef]
70. Becker, P.; Tebes, G.; Peppino, D.; Olsina Santos, L.A. Applying an improving strategy that embeds functional and non-functional requirements concepts. *J. Comput. Sci. Technol.* **2019**, *19*, 153–174. [CrossRef]
71. Kurtanović, Z.; Maalej, W. Automatically classifying functional and non-functional requirements using supervised machine learning. In Proceedings of the 2017 IEEE 25th International Requirements Engineering Conference (RE), Lisbon, Portugal, 4–8 September 2017; pp. 490–495.
72. Marchang, J.; Ibbotson, G.; Wheway, P. Will blockchain technology become a reality in sensor networks? In Proceedings of the 2019 Wireless Days (WD), Manchester, UK, 24–26 April 2019; pp. 1–4.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.