Preprints.org

Article

Not peer-reviewed version

Secure by Design Real-Time IoMT Architecture for e-Health Population Monitoring (RTPM)

Jims Marchang [*] , Jade McDonald , Solan Keishing , Kavyan Zoughalian , Raymond Mawanda , Corentin Delhon-Bugard , Nicolas Bouillet

Posted Date: 10 June 2024

doi: 10.20944/preprints202406.0403.v1

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

Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

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.

Article

Secure by Design Real-Time IoMT Architecture for e-Health Population Monitoring (RTPM)

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

[1] Computing Department, Sheffield Hallam University, Sheffield S1 1WB, UK
[2] Computer Science and Engineering, National Institute of Technology, Manipur, India
[3] Graduate school of science and engineering, Junia, Lille cedex, France
* Correspondence: jims.marchang@shu.ac.uk

Abstract: The healthcare sector has undergone a profound transformation, owing to the influential role played by IoMT (Internet of Medical Things) technology. However, there are substantial concerns over these devices' security and privacy-preserving nature. Current literature on IoMT tends to focus on specific security features like data confidentiality or data integrity or data availability or access control and most solutions are simulated and not tested in a real-world live network. This paper proposes a smart secure by design solution that safeguards user's data during health and wellbeing monitoring of patients locally (home, care-home, and hospital) and remotely. The proposed innovative solution is known as Secure by Design Real Time IoMT Architecture for e-Health Population Monitoring (RTPM) for smart hospitals and any healthcare monitoring management. In this system, keys can also be generated by the patient monitoring system independent to maintain high privacy standard and trust during the monitoring process and to enable the IoMT devices run independently even if the server is compromised and are made safe from external exploits to the client nodes. 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: confidentiality, integrity, availability, conducts authentication, protect from DoS attacks and prevent from non-repudiation attack of patient medical data and the devices in a real time, sensory data communication environment for live e-health monitoring. A secure communication is tested by capturing the live network traffic and the system's performance analysis of RTPM using different security algorithms with different key sizes of RSA, AES, and SHA shows that resource constraint low powered system can also successfully integrate with high-end state-of-the-art secure parameters and features and have the potential to support real time secure interaction. A stress test is also conducted to ensure that the system can withstand huge key sizes and different data types including multi-media information.

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

1. Introduction

Technology is ever-changing and it has revolutionised the way 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 caring for and monitoring patients in the realm of traditional healthcare. The authors of [1] stated that the introduction of high-speed data transmission and networking has allowed huge healthcare advancements. Sensors can now be utilised to monitor patients, allowing for timely and accurate

© 2024 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

diagnoses and immediate healthcare actions. It is noted that this progress has drastically improved the way patients can be cared for within the healthcare domain and in turn enhances their Quality of Life (QoL).

1.1. Introduction Internet of Things (IoT)

As we know, Kevin Ashton originated the term IoT in 1999. Kevin describes IoT as empowering systems to remove the dependency on humans being their only form of data input. He further explains that humans are error-prone and are highly inefficient in comparison to computers. Despite this, most of the data input used by computers comes directly from humans, in which IoT empowers the data collection and monitoring process. IoT is applied in various fields, including healthcare, smart framing, supply chain management, remote environmental monitoring, smart cities, and others [2]. IoT leverages M2M communication, replacing the need for humans to provide data input, which ensures scalability, reliability and accuracy. A significant advantage to IoT is its interoperability with many use cases and existing systems.

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, peacemaker implants, wearable devices, diabetes sensors, and others. IoMT is transforming patient treatment, enhancing the potential for successful patient recovery. 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. Projections indicate that by 2028, the IoMT sector is expected to surpass $187 billion, suggesting a promising path for the future of these devices [4]. 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 and Research Question

The 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 [5], IoMT devices must incorporate confidentiality, integrity, and authentication within their designs to ensure the privacy of the user data and the accuracy of data. As IoMT refers to medical devices the impact of a security incident could lead to permanent damage health consequences for patients and loss of life. This is a significant risk that must be dealt, with great care. It is 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. There is a clear research gap for more detailed research regarding IoMT security which aims to secure the system, including all the essential security objectives. Concentrating only on a few security aspects while omitting other security features does not ensure security by design and privacy by design frameworks. So, to tackle this issue, security and privacy aspects should be addressed from a holistic perspective. The proposed model will aim to ensure that the sensitive data of the patient is collected securely by the sensors, confidentially transmitted to the server by maintaining data integrity, and the storage at the sever is safeguarded from any form of unauthorised access. Thus, the paper is curated to aid secure by design and privacy by design solutions for smart hospital monitoring.

The unique contributions of this paper are firstly, the approach of securing the data and the IoMT system by design and the process in which the IoMT system authentication and authorization process is conducted. Secondly, the in-depth performance comparative study of secure integration of the interaction and engagement of the IoMT client with the user, IoMT server and the webserver. Thirdly, the self-healing process during network failure and data recovery. Fourthly, exploring different methods of alerting (email, display, sound etc.) for health and wellbeing events, ways of collecting diverse sensory information (movement, temp, humidity, light, air quality, proximity, pressure, multimedia etc.) to learn about the quality and wellbeing of the users. Lastly, exploring the best encryption and data signing processes to support real-time communication is some of the key highlights of this paper. The proposed system of this paper ensures that MAC spoofing is not possible because a unique ID (hash of user's registration data (ϒ), MAC address (∂), and a 32-bit random number (μ)) is used to detect and identify the participating devices, data tampering is impossible because of digital signature and non-repudiation attacks not possible because of signing using the sender's private key, and information disclosure is not possible due to high level of encryption and the key management policies are updated from time to time and DoS and DDoS attacks are averted by monitoring and allowing only authorised and authenticated devices into the monitoring system.

The rest of the paper is highlighted with Section 2 that study a state-of-the-art background discussion and detailed literature study on 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 result and discussion while Section 6 concludes the paper with future direction.

2. Background & Literature Study

This section covers the background of the Internet of Things and its transformative applications in healthcare systems. In addition, an extensive study is conducted on data security, data privacy, and security threats in IoMT applications and evaluate the current literatures in detail.

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. IoMT could and has reshaped the healthcare industry, bringing it forward into a new age of patient medical care. As stated in [6,7] 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. 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 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. 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 pushes 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. Which 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 industry [8,9]. Observation of lower ratios of nurses to patients within

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

hospital settings surpasses that of any other healthcare setting. 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.

2.3. Necessity of Data Security and Privacy

Reaping the great benefits these smart systems can provide brings a plethora of new challenges. There is a necessity for the production and collection of masses of data within smart systems, it is imperative that this data is 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, healthcare providers reputations, and trusts. Data mismanagement may lead to disciplinary measures against healthcare providers who fail to adhere to mandatory laws and regulations. Examples of these laws mandatory to follow when processing patient data include Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States of America and General Data Protection Regulation 2018 (GDPR) in the European Union. Non-compliance with such law can result in disciplinary action, fines, lawsuits, and loss of accreditation. Moreover, the accuracy and reliability of data is 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 [10] uncovers alarming statistics for security within healthcare. It is one of the top 10 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. For a better understanding of cyber-attacks within the healthcare industry, refer to Table 1 below outlining the attacks most likely to target the Healthcare industry (in no order), and their mitigations.

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

Cyber Attack Name	Description	Mitigation	Impact Example
SQL Injection	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 [11].
Zero-Day Exploits	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 [12].
Insider Threats	Staff or subcontractors with access to patient data might inadvertently cause harm or steal information.	Set access controls, monitor user behavior, 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 [13].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

Phishing	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 [14].
Password Attacks	Cracking passwords for unauthorised access; includes brute force or dictionary attacks.	Enforce strong password regulations, regular changes, complexity requirements, and establish two-factor authentication.	During a credential-stuffing attack on Magellan Health in 2020, 365,000 patients' information was stolen [15].
Malware	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 [16].
Supply Chain Attacks	Infiltrating healthcare systems through third-party hardware or software providers.	Monitor third-party vendors, enforce strict contracts, and conduct routine risk assessments.	Cyberattack on software developer SolarWinds compromised businesses, including healthcare providers in 2020 [17].
Social Engineering	Coercing individuals into disclosing private information or performing certain tasks.	Regular cybersecurity training, security awareness programs, and implementing security controls like spam filters and two-factor authentication.	Save the Children suffered a BEC attack in 2018, costing them £1 million due to a fraudulent money transfer [18].
Misconfiguratio n	Misconfiguring medical equipment or systems, making 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 demand submission at HMC in the US [19].
DDoS	Overwhelming healthcare systems with traffic, causing breakdown or inaccessibility.	Implement network segmentation, deploy DDoS mitigation services/hardware, and create a DDoS response strategy.	The WannaCry ransomware's 2017 spread was momentarily halted by a denial-of-service attack on its command-and-control servers [20].

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 [21], 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 it prevents access from unauthorised individuals. The system should ensure data Confidentiality (keeping information secret), Integrity (maintaining accuracy of information), and Availability (ensuring access to information by authorised users) [22].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

Enhanced levels of data confidentiality can be enforced where symmetric and asymmetric encryption keys can be used to allow varying levels of data security [23]. Research conducted by [24] has highlighted that high data latency can significantly impair the availability of data, emphasising the critical need for efficient 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 [25]. Security features are critical and have a significant impact on customers' trust and adoption of such technology [26]. 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 [27–29] and the system must ensure non-repudiation [30]. However, due to the device's constraints, it is very challenging to incorporate security features. So, the encryption mechanisms must support low-powered devices [31] and performance analysis of security features are studied in [32]. 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

There are different types of requirements including functional, security requirements, system requirements, tools needed, ethical consideration to successfully execute the design, development, and testing of the IoMT system.

3.1. Requirements

There are two main types of requirements: functional and non-functional. 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, but aims to enhance user experiences.

3.1.1. Key Functional Requirements for the System

- Encrypted communication between devices and server (IoMT and Webserver).
- Information Integrity checking implementation for message verification.
- Information avalability, Authentication of users and devices and non-repudiation functionality incorporation.
- Salting of the stored hashes to add next level of security.
- Data secure storage.
- Self-healing and no data loss during 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 LED and Buzzer sound to be inclusive in the interaction and engagement.
- User's participation during the securing process.

3.2. Security Constraints and Requirements

Incorporating security measures into resource-constrained devices poses significant challenges since the security mechnisms are influenced by computational limitations, memory constraints, and network restrictions. The authors of [38] also suggests that the IoT grapples with processing, storage, and network contraints. While solutions like the cloud could potentially address these constraints, however, they introduces additional security and privacy concerns since majority of the storage or

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

computation are done 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 contriants. It is crutial to maintain the following key aspects in the process of developing secure IoMT infrastructure.

Data Confidentiality: Ensure all patient data is protected to prevent privacy violations or exposure to unauthorised third parties.

Integrity: Ensure that patient medical data is tampered proof during the communication from the IoMT device to the server.

Authentication, Authorisation and Access Control: Ensure only authorised devices and users can join the network or begin communication to and from the server while participation is authorised and access of information is controlled.

Freshness: Ensure that real-time communication is achieved.

Non-Repudiation: Ensure data signing to validate where the data is 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.

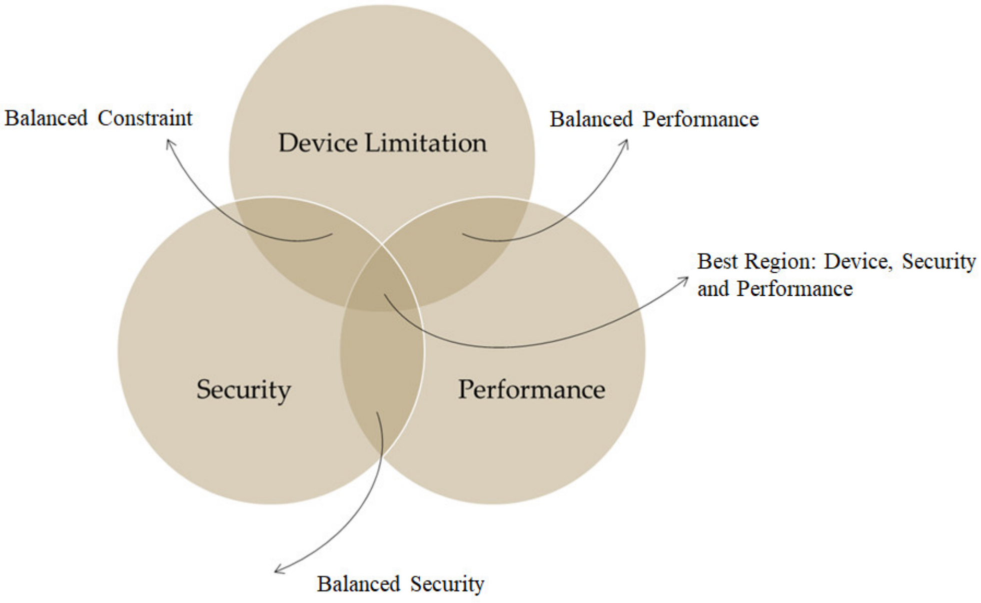


Figure 1. System Requirement.

3.3. System Requirements

This paper developed an IoMT device by integrating raw sensors with a Raspberry Pi based hardware computing systems for data pre-processing. The IoMT system should be securely connected with the IoMT server, and the webserver 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, lightweight. The Raspberry Pi is equipped with Sense HAT and the GrovePi+ sensors. The IoMT device, IoMT server and the webserver are all executed in an Unix based OS (Raspbian and Ubuntu).

3.4. Other Tools

Python 3 programming language for client server design and development and use XML, PHP, and Java Script for web-server development.

3.7. Testing Strategy

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

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 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 mesasage integrity and digital signature SHA 256 is used. During the testing the room windows and doors are opened occationally to test the air quality and blow on the heat and humidity sensing sensors to observe change in temperature and humidity readings. Also, move the IoMT device and appraoch the device to test the functions of the alerting and evidence collection aspects.

4. Proposed System & 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 the wellbeing in two-folds 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, display message with LCD, buzzer, LED). Only the sensors related to the quality and wellbeing of the users are used in this work. The proposed RTPM is a secure by design solution that protects the data source (IoMT device), data transmission, and authorised every user participating in the system to support auditing and accounting. The proposed system addressed 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) interact securely through a combination of RSA, AES, and SHA algorithms.

Data Integrity: Every data generated by the IoMT client is 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 controlling access.

System Recovery and Self-Healing Network: If the client is disconnected, the last data block sent is remembered and continues sending the data from the last point of failure 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 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).

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. for monitoring physical intrusion.

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

In addition, the paper conducts an in-depth performance comparative study of secure integration of the interaction and engagement of the IoMT client with the user, IoMT server and the web server. This study enlightens the researching community to know 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 and be able monitor the ambient space for wellbeing monitoring (movement, light, pressure, magnetic flux, air quality etc.) The system also monitors and alerts

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

surrounding people with messages via LCD, buzzer, LED 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, nurse, carer, friends, and family) depending on the condition of the patients and the environment in which the patient is monitored as shown in Figure 2. The user needs to hold the temperature and moisture/humidity sensor for data collection and the rest of the wellbeing data of the environment of the patient is continuously monitored at the same time. If the data doesn't change then, the sensory information is not transmitted to the server to reduce system overhead, however, if the data remains constant for over 5 minutes, then the data is pushed to the server to ensure the system's liveness. The system can detect if there is movement, if the device is disturbed, the brightness of the room is changed, or if the air quality and pressure of the room changes. Such a system is perfect for monitoring population health in general and is perfect for a situation like Covid-19 pandemic situation. The system can be deployed locally in a hospital and remote care or home environment. The architecture ensure that the IoMT device is securely registered and authorised, the data is transmitted securely (confidentiality and integrity maintained), data source 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 securely locked.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

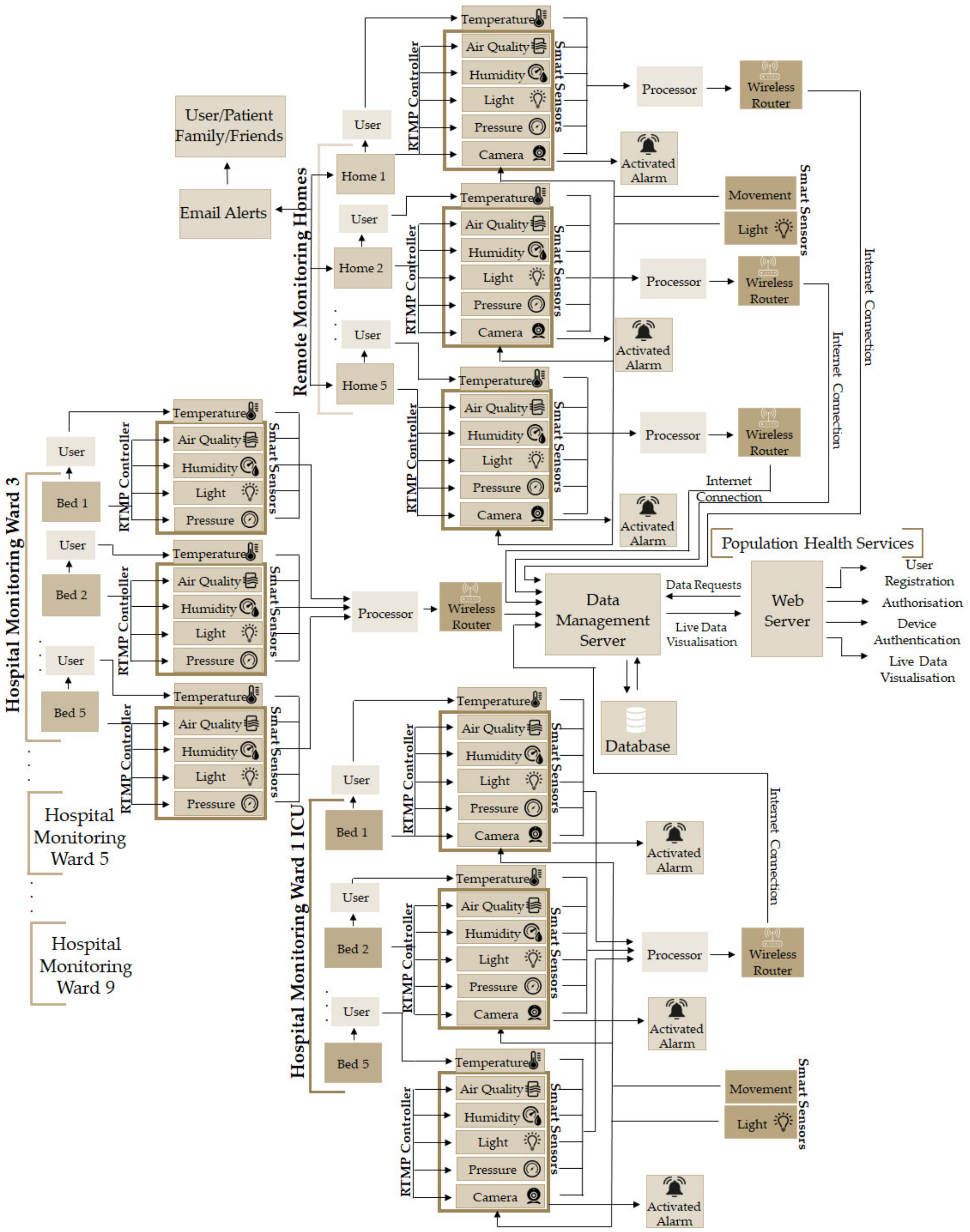


Figure 2. Proposed IoMT monitoring Architecture.

4.2. RTPM Controller at the Client

The IoMT device is activated with 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 heart rate, ECG and Oxygen level could not be integrated. The system continually monitor the user and its environment as shwn in Figure 3 and the system records every events and evidences inlcuding errors to monitor the issues and identify the reasons of the failures of the system. The controller monitors the events and activities of all the four activity strands and alert the concern and relevant stackholders including the people around the room if they come too close or move the device or even try to steal. In such event, an evidence is collected in the form of movement detection and snapshots of the environment is captured with the camera and the evidece are securely transmissted to the server for investigation and service quality monitoring (knows who touch the device, when and how often etc.).

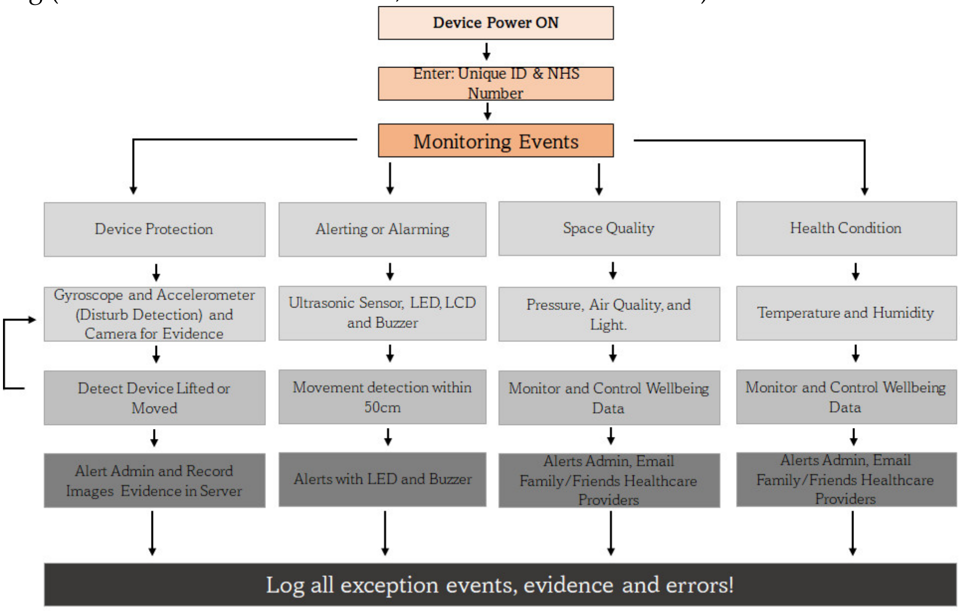

Device Power ON
Enter: Unique ID & NHS Number
Monitoring Events
Device Protection
Alerting or Alarming
Space Quality
Health Condition
Gyroscope and Accelerometer (Disturb Detection) and Camera for Evidence
Ultrasonic Sensor, LED, LCD and Buzzer
Pressure, Air Quality, and Light.
Temperature and Humidity
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 3. RTPM Controller Architecture at the client.

4.3. RTPM User, Device, and Key Management

The keys are managed as shown in Figure 4. 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, and the public key is shared with the server and the server does likewise. This doesn’t 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 has to register to the webserver 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 nonce (μ)= SHA256(32-digit random number) and these data are used for the IoMT identification and authenticate during the device connection to the server as shown in Figure 4. The unique ID used during the device identification = SHA256(ϒ+∂+μ) and since its raw data are with the server, it can validate the hash value and authenticate it. Thus, in the first step user registration is conducted as shown in Figure 5 and Figure 6 elaborates how the authorisation process is conducted to verify the authenticity of the user. Figure 7 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 4. 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 the AES 256 which is provided by the IoMT server and signing the data using SHA 256 as explained in step 6 of Figure 4 where 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 and the IoMT server's private key = RSA PriK-S and the public key is = RSA PubK-S.

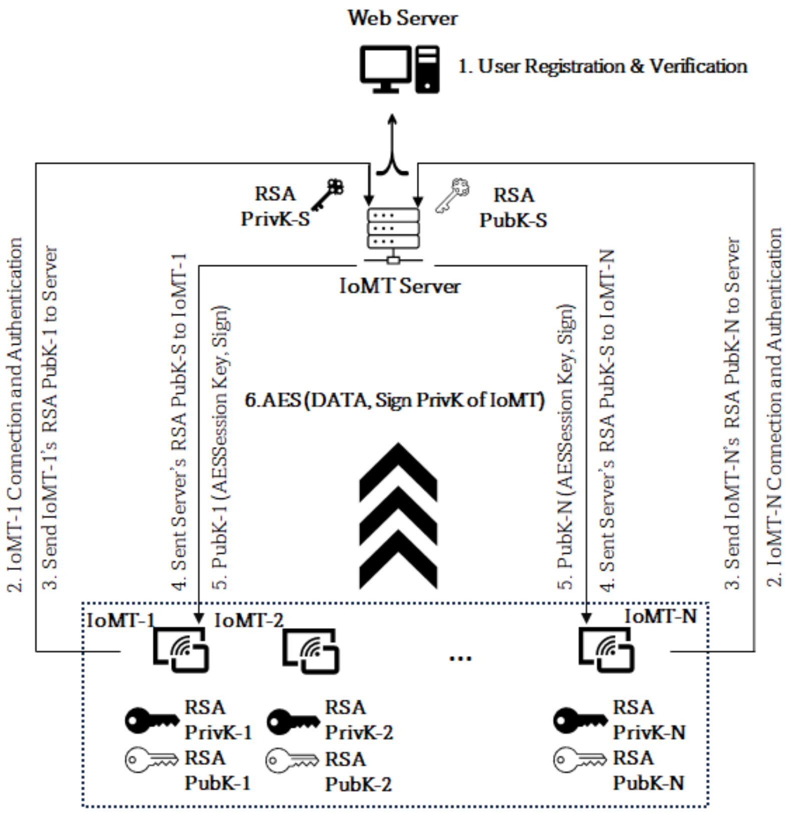
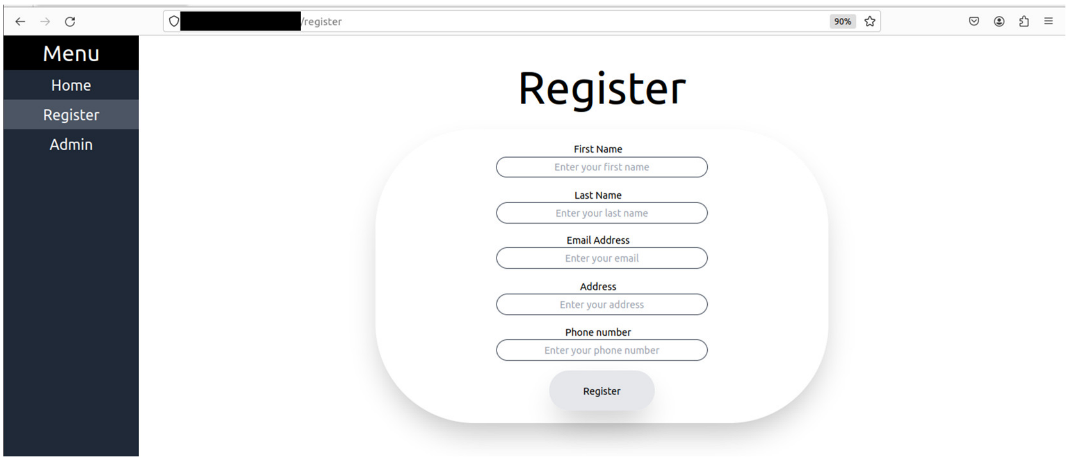

Web Server
1. User Registration & Verification
RSA PrivK-S
RSA PubK-S
IoMT Server
2. IoMT-1 Connection and Authentication
3. Send IoMT-1's RSA PubK-1 to Server
4. Sent Server's RSA PubK-S to IoMT-1
5. PubK-1 (AESSession Key, Sign)
6.AES(DATA, Sign PrivK of IoMT)
5. PubK-N (AESSession Key, Sign)
4. Sent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



Register

First Name
Enter your first name

Last Name
Enter your last name

Email Address
Enter your email

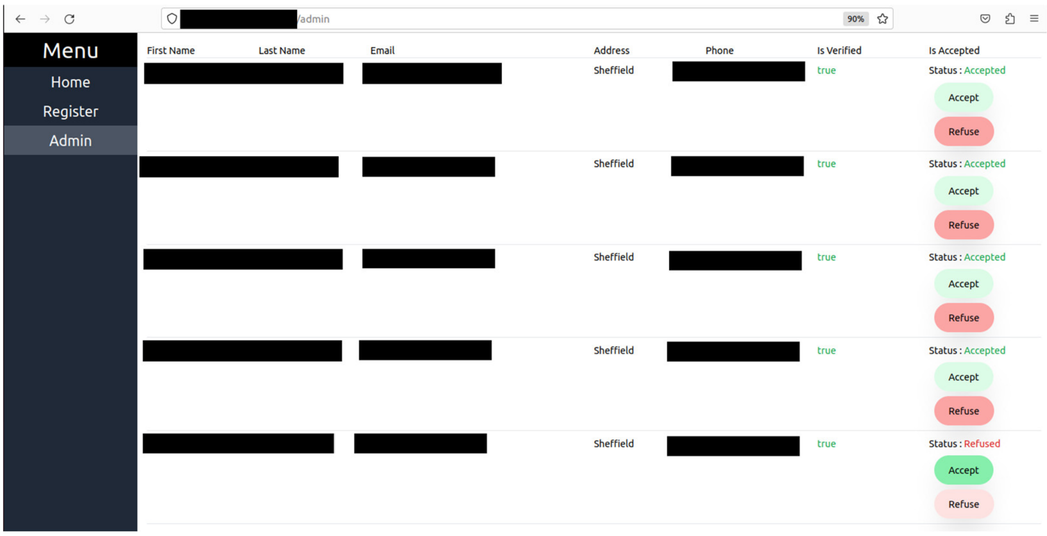
Address
Enter your address

Phone number
Enter your phone number

Register

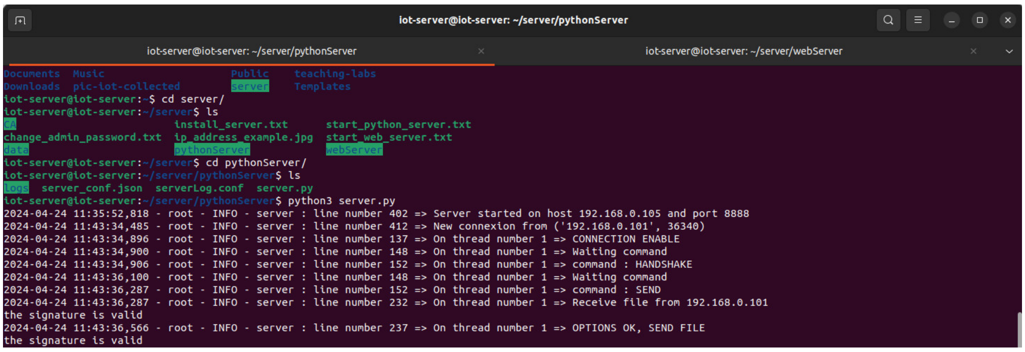
Figure 5. User Registration for Monitoring.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1



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

Figure 6. 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 7. 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 is communicated securely, the integrity of the data is preserved, strong authentication and access control, accounting and logging of every exception and error are conducted for incident response and recovery, the 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 wellbeing-related data. The proposed system interacts and engages between 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 IoMT client (Raspberry Pi 4) with a configuration, Broadcom BCM2711 SoC with a 1.8 GHz, 64-bit quad-core ARM Cortex-A72 processor with 4GB RAM and the IoMT server executing with 64-bit, Intel Core i7, CPU @2.6GHz with 32GB RAM. The system is tested with various key sizes (standard and above) to select the best key sizes for performing real-time

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

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 exponential time as the key size increases. The AES key generation time encryption time or decryption time takes only a few milliseconds irrespective of the key sizes (128-bit, 192-bit, or 256-bit) while the RSA takes a little less than a second only for those key sizes below 2048-bit key size for key generation, but takes some seconds to minutes for key sizes RSA 4096 and above respectively. However, the RSA method of encryption takes from around 0.01s to 0.07s when the key size increases from RSA 1024 bit to RSA 8192 bit. 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 done 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: Every data generated by the IoMT client is signed and the integrity of the data is preserved using SHA-256 along with the private of the sender to avoid any form of non-repudiation attack. Creating a digital signature of the IoMT data takes 0.0011s to 1.03s when the RSA 1024-bit key and RSA 8192-bit key respectively are used. As expected as the key size increases the digital verification takes longer, but it is more of a linear and not exponential. Since the paper uses an RSA 2048-bit key, it takes 0.04s for signing and 0.0008s 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 conducting any form of DoS or DDoS attack. The proposed system authorised 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 and is provided to add in the IoMT client as a unique ID = SHA256(ϒ+∂+μ) 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 request (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 done 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 every data should be delivered. So, in this system is 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 continues sending the data 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 every data that is acknowledged by the server is set to 1 to realise what is 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). It is to support and update the wellbeing of the user to the carers and near ones. 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 and a red LED and 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 done 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 8 shows a warning message while Figure 9 alert message is triggered when someone comes too close to the device and Figure 10 shows an activation of the camera when someone attempts to take or move the IoMT device. These systems are necessary to alert the surroundings and also connect with the concern stackholders of the user. s

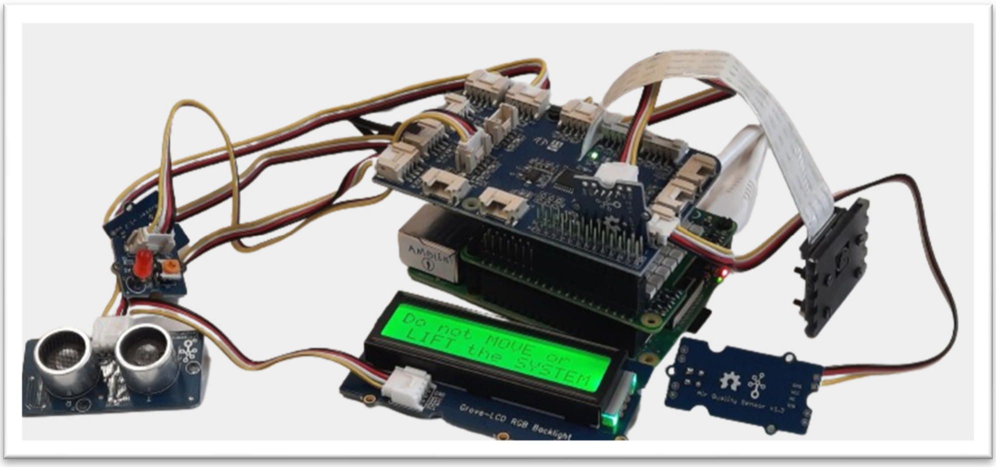


Figure 8. Warning Message so that the device is not moved.

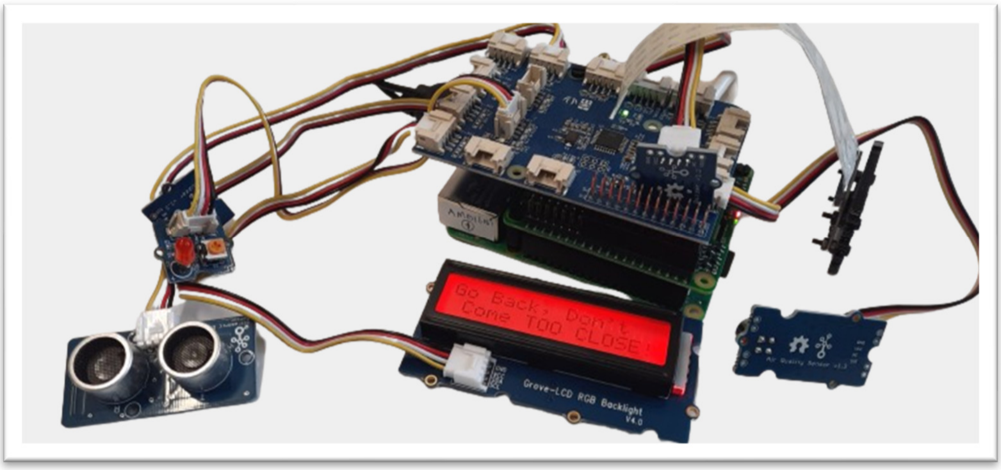


Figure 9. Warning when coming too close.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

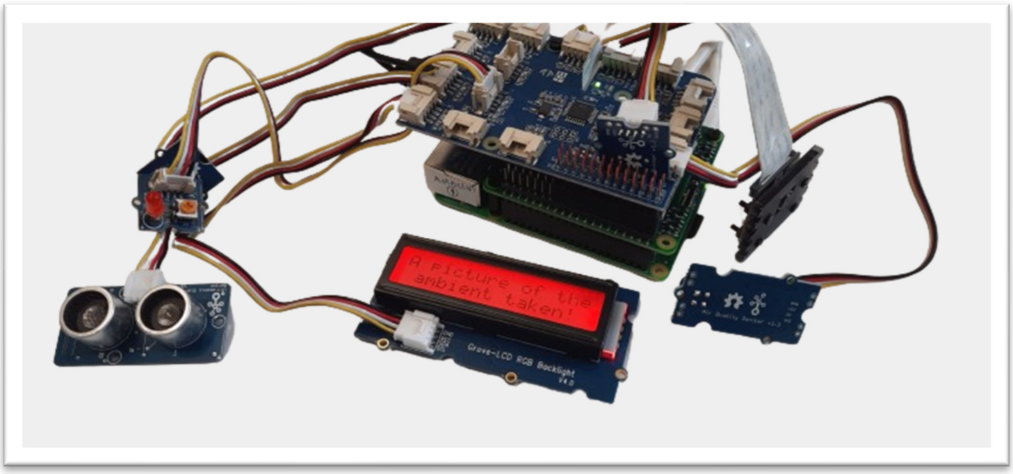


Figure 10. Capturing evidence if the system is moved.

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 sensor and humidity sensors and the results are shown in Figure 11. The spikes in the results are the results of blowing warm air through the mouth which guarantees a 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 seconds 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 minutes with no change in the data reading to ensure that the connection is live.

Figure 12 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 is decreased and it happens when 5 people sat around the IoMT sensor (more released of CO2) and the lower reading value of air quality occurring towards the end of the reading shows that the air quality is improved and it was triggered by the opened windows. The distance between the proximity sensor and the wall was measured at 110cm, and the spikes are the result of introducing a human hand movement towards the proximity sensor at different times.

The light and noise levels are measured and recorded in Figure 13. The reading of above 600 Lux is due to the instruction of more lighting around the sensor and when the reading goes down is/is due to the closing of window curtains. The normal lab sound record is 65 Db and 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.

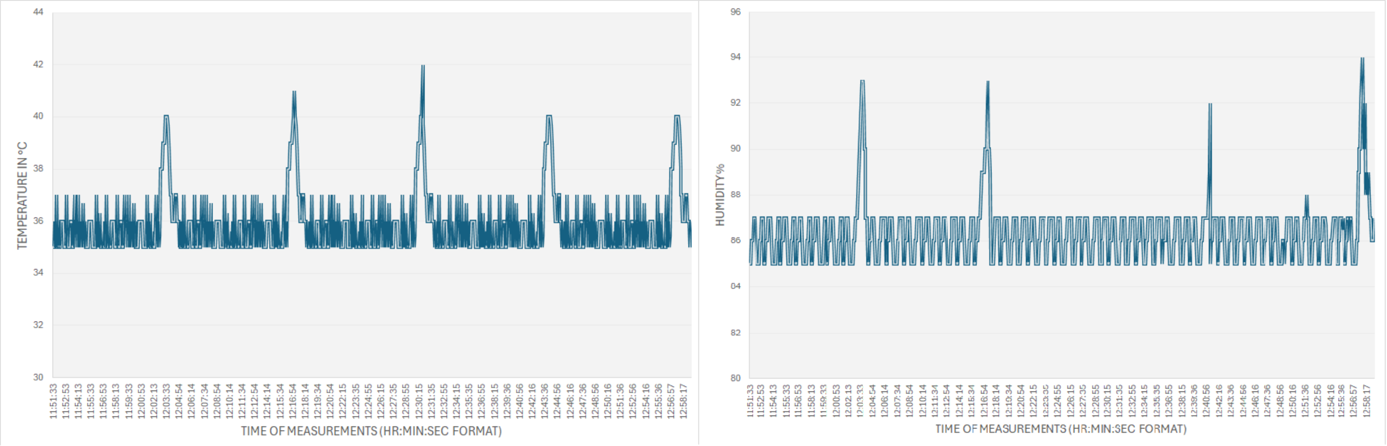


Figure 11. The Body Temperature and Moisture Level.

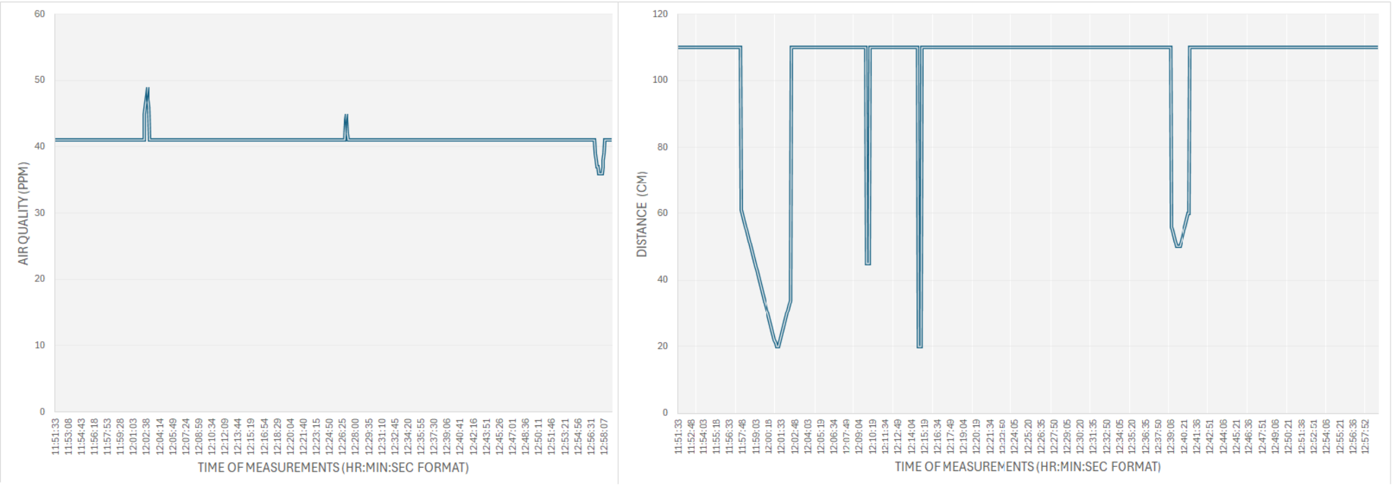


Figure 12. Air Quality of the Room and Movement Monitoring.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

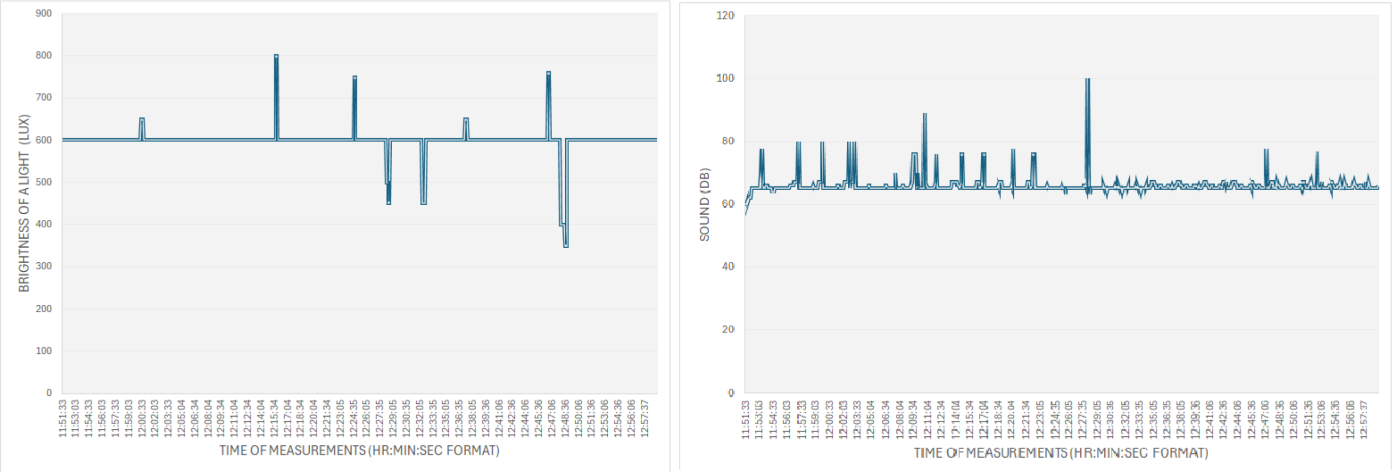


Figure 13. Lighting and noise monitoring.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

6. Conclusions

The 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 and 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-bit or above because such key generation with a processing power of @1.8GHz takes around 8-9s, and when it is RSA 8192-bit key, it takes around 3 minutes on average and when it is of such a huge key size along with SHA256 creating a digital signature and signing takes over 1s. So, to meet real-time requirements, it is ideal to adopt the signing process using the RSA 2048 for low computation power, however, due to the lightweight nature of the AES, any secure key sizes from 128-bit key to AES 256-bit can be adopted for real-time communication. So, it is recommended to use RSA 2048, and 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 one should not outweigh the other parameter otherwise, the system will not be usable. The developed system ensures that MAC spoofing is not possible because a unique ID is used to detect and identify the device, data tampering and repudiation attacks not possible because of digital signature and signing using the sender's private key, and information disclosure is not possible due to high level of encryption and update of key management policies and DoS and DDoS attacks are averted by monitoring and allowing only authorised and authenticated devices into the monitoring system.

The developed system needs to be tested against the acceptance and adoption aspects with potential users in hospitals and care homes to study the impact of such solutions and that will be part of future work. The system also needs to incorporate other aspects of secure-by-design features like automatic detection of intrusion and threats, security controls, application failure recovery, patch management, etc.

Supplementary Materials: None.

Author Contributions: Dr. Jims Marchang i.e. the corresponding author along with Solan Keishing designed and developed the framework and conducted the implementation, testing, and validation of the secure IoMT system. Jade McDonald, Kavyan Zoughalian, and Raymond Mawanda supported the work by conducting a critical literature study and supporting drafting the paper and drawing the diagrams and figures. Corentin Delhon-Bugard and Nicolas Bouillet supported Dr. Jims Marchang and Solan Keishing in developing, implementing, and testing the IoMT client, IoMT server, and web server of the system.

Funding: This research was funded by Sheffield Hallam University.

Data Availability Statement: The data is collected using the IoMT framework from a laboratory of Computing Department of iSec CyberNet and it is not appropriate to share the raw data. The source code can be shared for those who want to test. Data 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 due to (specify the reason for the restriction).

Acknowledgments: We would like to thank the Sheffield Hallam University for providing us the necessary fund for buying IoMT devices, use cybersecurity lab resources for developing, hosting web-server and testing in a real world lab environment.

Conflicts of Interest: Nothing to declare.

References

1. Mohanta, B., Das, P., & Patnaik, S. (2019). Healthcare 5.0: A Paradigm Shift in Digital Healthcare System Using Artificial Intelligence, IOT and 5G Communication. 2019 International Conference on Applied Machine Learning (ICAML). https://doi.org/10.1109/icaml48257.2019.00044

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

2. Ashton, K. (2009). That "Internet of Things" Thing. In That "Internet of Things" Thing -RFID Journal. https://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf
3. Scarpato, N., Pieroni, A., Nunzio, L. D., & Fallucchi, F. (2017). E-health-IoT Universe: A Review. International Journal on Advanced Science, Engineering, and Information Technology, 7(6), 2328. https://doi.org/10.18517/ijaseit.7.6.4467
4. Internet of Medical Things [IOMT] Market Size and Growth, 2028. (2024, April 8). Retrieved April 24, 2024, from https://www.fortunebusinessinsights.com/industry-reports/internet-of-medical-things-iomt-market-101844
5. Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., Iqbal, W., Rashid, I., & Yaseen, A. (2018). Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. IEEE Access, 6, 464–478. https://doi.org/10.1109/access.2017.2767561
6. Vishnu, S., Ramson, S. R. J., & Jegan, R. (2020). Internet of Medical Things (IoMT) - An overview. 2020 5th International Conference on Devices, Circuits and Systems (ICDCS). https://doi.org/10.1109/icdcs48716.2020.243558+++-https://doi.org/10.1109/icdcs48716.2020.243558+++-
7. Malasinghe, L. P., Ramzan, N., & Dahal, K. (2017). Remote patient monitoring: a comprehensive study. Journal of Ambient Intelligence and Humanized Computing, 10(1), 57–76. https://doi.org/10.1007/s12652-017-0598-x
8. Tabatabaei, S. M., Kasrineh, M. R., Sharifzadeh, N., & Soodejani, M. T. (2021). COVID-19: an Alarm to Move Faster towards "Smart Hospital." Online Journal of Public Health Informatics, 13(1). https://doi.org/10.5210/ojphi.v13i1.11515
9. Michard, F., Saugel, B., & Vallet, B. (2020). Rethinking the post-COVID-19 pandemic hospital: more ICU beds or smart monitoring on the wards? Intensive Care Medicine, 46(9), 1792–1793. https://doi.org/10.1007/s00134-020-06163-7
10. [10]IBM Security X-Force Threat Intelligence Index 2024. https://www.ibm.com/reports/threat-intelligence
11. BBC News. (2014, August 18). Community Health Systems data hack hits 4.5 million. BBC News. https://www.bbc.co.uk/news/technology-28838661
12. Zetter, K. (2016, January 13). Hacking team's leak helped researchers hunt down a Zero-Day. WIRED. https://www.wired.com/2016/01/hacking-team-leak-helps-kaspersky-researchers-find-zero-day-exploit/
13. Staff, D. R. (2023, December 11). Former NY hospital employee admits to stealing colleagues' data. https://www.darkreading.com/cyberattacks-data-breaches/former-ny-hospital-employee-admits-to-stealing-colleagues-data
14. Anthem pays OCR $16 million in record HIPAA settlement following largest U.S. health data breach in history | Guidance Portal. (n.d.). https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach
15. Davis, J. (2021, October 19). Magellan Health Data breach victim tally reaches 365K patients. HealthITSecurity. https://healthitsecurity.com/news/magellan-health-data-breach-victim-tally-reaches-365k-patients
16. Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International journal of advanced research in computer science, 8(5), 1938-1940.
17. Lazarovitz, L. (2021). Deconstructing the solarwinds breach. Computer Fraud & Security, 2021(6), 17-19.
18. Muncaster, P. (2024, April 28). Save the Children hit by $1m BEC scam. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/save-the-children-hit-by-1m-bec/#:~:text=Phil%20Muncaster&text=The%20attacker%20managed%20to%20access,center%20solar%20panels%20in%20Pakistan.
19. Townsened, C. (2019, January 30). Why data security has become a priority for healthcare professionals. United States Cybersecurity Magazine. https://www.uscybersecurity.net/healthcare/
20. Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International journal of advanced research in computer science, 8(5), 1938-1940.
21. Martani, A., Geneviève, L. D., Elger, B., & Wangmo, T. (2021). 'It's not something you can take in your hands'. Swiss experts' perspectives on health data ownership: an interview-based study. BMJ Open, 11(4), e045717.
22. Zhang, C., Xia, J., Yang, B., Puyang, H., Wang, W., Chen, R., ... & Yan, F. (2021, November). Citadel: Protecting data privacy and model confidentiality for collaborative learning. In Proceedings of the ACM Symposium on Cloud Computing (pp. 546-561).
23. Simmons, G. J. (1979). Symmetric and asymmetric encryption. ACM Computing Surveys (CSUR), 11(4), 305-330.
24. Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., & Wu, D. O. (2020). Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Communications Surveys & Tutorials, 22(4), 2462-2488.
25. Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal, 21(4), 574-588.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 June 2024 doi:10.20944/preprints202406.0403.v1

26. AlHogail, A. (2018). Improving IoT technology adoption through improving consumer trust. Technologies, 6(3), 64.
27. Dzissah, D. A., Lee, J. S., Suzuki, H., Nakamura, M., & Obi, T. (2019). Privacy enhanced healthcare information sharing system for home-based care environments. Healthcare informatics research, 25(2), 106.
28. Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications, 153, 311-335.
29. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. Ieee Access, 6, 20596-20608.
30. Yeh, K.-H. (2016). BSNCare+: A Robust IoT-Oriented Healthcare System with Non-Repudiation Transactions. Applied Sciences, 6(12), 418. https://doi.org/10.3390/app6120418app6120418
31. Tsai, K.-L., Huang, Y.-L., Leu, F.-Y., You, I., Huang, Y.-L., & Tsai, C.-H. (2018). AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments. IEEE Access, 6, 45325–45334. https://doi.org/10.1109/access.2018.2852563
32. Moosavi, S. R., Nigussie, E., Levorato, M., Virtanen, S., & Isoaho, J. (2018). Performance Analysis of End-to-End Security Schemes in Healthcare IoT. Procedia Computer Science, 130, 432–439. https://doi.org/10.1016/j.procs.2018.04.064

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.