Security Enhanced Cloud-Based Remote Patient Monitoring System with Human Digital Twin and OPC UA

University of Turku
Department of Computing
May 2024
Jolly Trivedi

Supervisors:
Tahir Mohammad (Univeristy of Turku)
Jouni Isoaho (University of Turku)

UNIVERSITY OF TURKU
Department of Computing

Author: Jolly Trivedi
Title: Security Enhanced Cloud-Based Remote Patient Monitoring System with Human Digital Twin and OPC UA
Number of Pages: 99

July 2024

The introduction of Human Digital Twin (HDT) technology marks a new era of personalized healthcare, with unparalleled prospects for Remote Patient Monitoring (RPM). This thesis presents a novel architecture for securing patient data and enhancing personalized healthcare in RPM, addressing the critical need for robust cybersecurity measures in RPM systems.
The proposed architecture seamlessly combines healthcare wearable devices with the OPC Unified Architecture (OPC UA) protocol, ensuring secure and interoperable communication. In the proposed architecture, a multi-layered security strategy is implemented by using pseudonymization techniques that not only safeguard data but also aid in preserving its utility for personalized treatment. This pseudonymized data is then transferred to the cloud via Azure IoT Hub, creating a secure pipeline for sensitive health information. The journey culminates in Azure Digital Twin, where advanced analytics and predictive modeling open the doors for truly personalized healthcare.
This design distinguishes itself by adhering to NIST SP 1800-30B criteria. The goal is not only to construct a secure system but also to provide a framework that can adapt to emerging threats. The efficacy of this technique is proved through thorough testing, including a Chi-Square study that compares the proposed RPM to current systems. Testing and statistics reveal the proposed design outperforms existing RPM systems. This study proposes a robust, scalable, and standards-compliant solution to one of healthcare's most serious issues. It is more than simply an architecture. It is also a road map for the future of secure, personalized remote patient care. To verify the suggested system's scalability and real-world performance, more investigation and pilot testing are required.

Keywords : Security, Privacy, Remote Patient Monitoring, PHI, OPC-UA, Human digital twin, azure IoT, Azure Digital twin, Cloud security, Pseudonymization, Federated learning

Contents

List of Figures

List of Tables

List of acronyms

BLE Bluetooth Low Energy

DoS Denial of Service

ePHI electronic protected health information

GDPR General Data Protection Regulation

HDT Human Digital Twin

HIPAA Health Insurance Portability and Accountability Act

IOT Internet Of Things

LoRaWAN Long Range Wide Area Network

MQTT Message Queuing Telemetry Transport

NCCoE National Cybersecurity Center of Excellence

NIST National Institute of Standards and Technology

OPC UA OPC Unified Architecture

PHS Personalized Healthcare Services

RPM Remote patient monitoring

TLS Transport Layer Security

1 Introduction

Personalized medicine has revolutionized healthcare through technological advancements. Among these developments, Human Digital Twin (HDT) technology has emerged as a game-changing way to improve remote patient monitoring (RPM). This thesis investigates the integration of HDT technology alongside OPC UA (OPC Unified Architecture) with a strong architecture aimed at securing patient data and enhancing the quality of personalized healthcare.

Remote patient monitoring (RPM) has gained significant traction in recent years, driven by the need for efficient and effective healthcare delivery. Wearable devices enable continuous vital sign monitoring, allowing timely interventions and reducing hospital visits. A systemic review by Irina et al.[1] highlights that RPM has the potential to improve the quality of care by providing more frequent communication, management, and follow-up, which may lead to better health outcomes for patients with heart failure. However, digital health technologies raise data security and privacy concerns. According to the National Cybersecurity Center of Excellence (NCCoE), "the increasing use of telehealth and RPM systems has made them attractive targets for cyberattacks, necessitating robust security measures" [2].

HIPAA mandates safeguarding electronic protected health information (ePHI) to maintain patient trust and regulatory compliance. It requires administrative, physical, and technical standards to be adopted to protect the confidentiality and integrity of electronic PHI [3].

HDT technology creates virtual patient representations, integrating wearable device data, health records, and genomic information. This comprehensive view enables accurate diagnosis, treatment, and health event prediction. The proposed architecture combines HDT with OPC Unified Architecture protocol, ensuring secure, interoperable device communication. This integration aligns with NIST SP 1800-30B guidelines [2] for a secure RPM ecosystem, mitigating data breach risks.

By leveraging HDT, healthcare providers can monitor individual health continuously, identify issues early, and tailor interventions. This thesis aims to contribute to next-generation patient care, presenting a framework addressing RPM security concerns while enhancing architectural design in the context of personalized healthcare delivery. The proposed architecture encompasses the overall structure, integration, and high-level design principles required to securely transfer and process healthcare wearable device data using OPC UA, Azure IoT Hub, and Azure Digital Twin. The work aspires to shape a secure, effective future in healthcare delivery.

1.1 Problem Statement

The demand for remote patient monitoring (RPM) systems in modern healthcare is growing for a variety of reasons, including an aging population, an increase in the prevalence of chronic diseases, and a desire for personalized care. RPM allows doctors to keep an eye on patients between clinic visits or in situations when in-person care is not feasible. Patients with long-term health issues, including diabetes, heart disease, and asthma, especially benefit from this ongoing monitoring. Additionally, RPM is being utilized more frequently in hospital-at-home programs, which offer in-home care for higher acuity diseases backed by ongoing biometric monitoring and telemedicine visits. Ensuring patient safety in this configuration and providing appropriate instruction on device operation are critical. Clinical misdiagnosis or a failure to recognize when a patient needs care from a physician are potential dangers.

However, traditional RPM systems face several challenges, including:

1. **Privacy Concerns:** Centralized data storage and processing raise significant privacy concerns, as sensitive patient health data may be vulnerable to unauthorized access or breaches.

2. **Data Interoperability:** Heterogeneity in data formats and communication protocols across different healthcare devices and systems complicates data integration and interoperability, hindering seamless information exchange.

3. **Real-time Decision-making:** Timely and accurate decision-making is critical in healthcare, especially for identifying and addressing emergent health issues. Delays in data transmission and processing can impede the ability to provide timely interventions.

4. **Scalability and Efficiency:** As the volume and complexity of healthcare data continue to grow, traditional centralized approaches may struggle to scale efficiently, leading to performance bottlenecks and resource constraints.

1.2 Research Questions

1. What communication protocols and encryption techniques are suitable for securing the transmission of data between the healthcare wearables/medical devices and the Digital Twin in a Remote monitoring system?

2. How can OPC UA be leveraged to ensure secure communication between medical devices and the cloud?

3. What are the advantages of the Human Digital Twin in Healthcare?

4. How does the proposed security architecture perform in terms of security effectiveness?

1.3 Objectives

The thesis proposes an architecture to overcome the aforementioned difficulties by creating a novel framework that makes use of Azure IoT Hub, Azure IoT Digital Twin technology, OPC UA standards and protocols, and Digital Twin Definition Language (DTDL) for RPM. The specific objectives are as follows:

1. Develop a secure and scalable architecture for RPM that integrates HDT technology for real-time monitoring, analysis, and prediction.

2. Evaluate the performance of the proposed architecture against existing RPM systems using synthetic heart rate data.

3. Determine and deal with any challenges or constraints that may arise when the suggested architecture is put into effect.

1.4 Thesis Structure

This thesis is structured into eight distinct chapters, each designed to provide a comprehensive exploration of the proposed architecture for securing patient data and enhancing personalized healthcare in remote patient monitoring (RPM) systems. The first chapter is titled Introduction. The introduction chapter sets the stage for the thesis by providing an overview of the research topic and its significance in the context of healthcare. It highlights the growing importance of remote patient monitoring and the critical need for secure and personalized healthcare solutions. The chapter also presents the research objectives and outlines the structure of the thesis.

Chapter 2 delves into the theoretical foundations and existing research relevant to the proposed architecture. It explores the concepts of OPC UA, Human Digital Twin (HDT) technology, various secure communication protocols, Azure Cloud, and

their applications in healthcare. It also discussed various cyber attacks in healthcare. The literature review examines previous studies on remote patient monitoring, data security, and personalized medicine, providing a solid basis for the research conducted in this thesis.

The methodology chapter outlines the research approach and the various techniques employed to develop and evaluate the proposed architecture. It describes the proposed architecture and its various components. Chapter 4 focuses on the practical implementation of the proposed architecture. It details the integration of healthcare wearable devices with the OPC Unified Architecture (OPC UA) protocol, the implementation of pseudonymization techniques, and the data transfer process to Azure IoT Hub and Azure Digital Twin. The chapter also addresses the challenges encountered during the implementation phase and the strategies used to overcome them.

The experimental evaluation chapter presents the results of the various tests and analyses conducted to assess the effectiveness of the proposed architecture. It includes the Chi-Square test comparing the security features and performance of the proposed RPM system against existing solutions. The chapter also discusses the use of synthetic data based on existing clinical heart rate data to validate the architecture's ability to enhance personalized monitoring and predictive analytics. Chapter 6 critically analyzes the findings of the research and discusses their implications for the healthcare industry. It highlights its unique features and advantages. The chapter also addresses the limitations of the research and the potential challenges associated with the implementation of the proposed architecture in real-world settings.

The future work chapter outlines several key areas for further investigation that can enhance the proposed architecture and expand its applications in healthcare. It discusses the integration of advanced privacy-preserving techniques such as dif-

ferential privacy and federated learning, as well as the implementation of artificial intelligence to improve predictive analytics capabilities. This chapter emphasizes the importance of ongoing research and collaboration in addressing the evolving challenges in healthcare. The conclusion chapter summarizes the key findings of the thesis and reiterates its contributions to the field of secure and personalized healthcare in remote patient monitoring. It highlights the significance of the proposed architecture in improving patient outcomes and reducing healthcare costs. The chapter also emphasizes the need for continuous innovation and the potential for future research to further enhance the effectiveness of remote patient monitoring systems.

The research was done in mainly 3 stages as mentioned in Figure 1.1

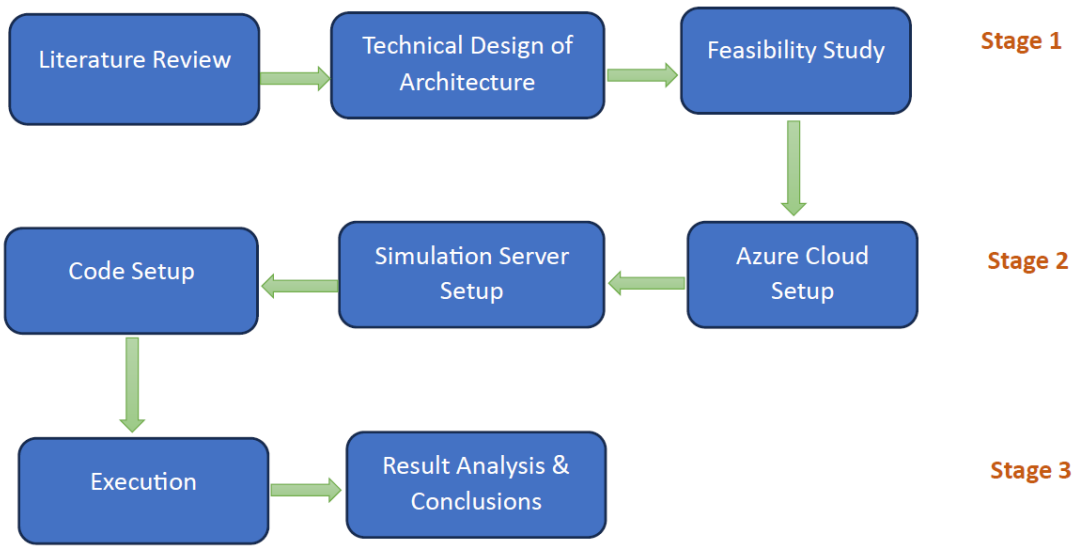

Figure 1.1: Thesis Structure

2 Concepts and Literature Review

2.1 IoMT (Internet Of Medical Things)

Computer scientist Kevin Ashton coined the phrase "Internet of Things (IoT)" in 1999. Internet of Medical Things (IoMT) is a subset of IoT that focuses on the healthcare industry. The Internet of Medical Things (IoMT) developed as the Internet of Things (IoT) concept matured due to the interconnectedness of medical devices, software, and healthcare systems. Through the use of technology like healthcare wearables, wearable health monitors, remote patient monitoring devices, and smart medical equipment, IoMT promises to enhance patient outcomes, expedite healthcare procedures, and promote individualized treatment.

The three main uses of IoMT are clinical efficiency, personal healthcare management, and remote patient monitoring. IoMT devices make it possible to continuously monitor patients' health, giving real-time data that can result in quicker actions and more accurate diagnoses. With the use of health tracking and feedback technologies, patients can take an active role in their healthcare experience. IoMT lowers healthcare expenses by reducing readmissions and hospital stays. Large-scale data generation results in tailored treatment regimens, predictive analytics for potential health hazards, and better decision-making.

Through improved patient outcomes, disease prevention, patient engagement, and access to healthcare services, IoMT plays a critical role in improving health-

care. IoMT has revolutionized patient care, treatment monitoring, and healthcare operations, which has had a huge impact on the industry. Proactive treatment, cost reduction, emergency care, remote patient monitoring, and improved health tracking have all benefited from it. IoMT has emerged as a key component of contemporary healthcare, providing a plethora of applications that tackle pressing issues in the field, particularly in times of crisis such as the COVID-19 outbreak.

According to Razdan et al., [4], the Internet of Medical Things (IoMTs) will revolutionize present healthcare systems by allowing healthcare providers to link and monitor every medical gadget remotely via the Internet. Figure 2.1 illustrates an example of an Internet of Medical Things (IoMT) where patient vitals are gathered using sensor devices and transmitted to the IoMT apps via the Internet, as covered in the article. The medical personnel and healthcare professionals receive the information, and they respond to the patients who require it.

Remote patient monitoring (RPM) has advanced greatly as a result of the Internet of Medical Things (IoMT), which uses linked devices to improve healthcare. IoMT makes it possible for medical professionals to remotely collect real-time patient data, facilitating ongoing observation and analysis outside of conventional hospital settings. Through the use of this technology, patients' problems can be better understood in between appointments, resulting in more efficient and customized therapy. Personalized healthcare, expedited hospital treatments, cost-effective medical solutions, and enhanced patient comfort are all made possible by IoMT, according to an article by Razdan et al. [4]. It further claims that IoMT entails the gathering of patient vitals via sensor devices and the online sharing of this data with medical professionals and staff. It goes on to say that the response from medical professionals has improved due to patient monitoring systems.

Razdan et al. [4] discussed critical layers of IoMT and described the importance of the cloud layer in IoMT, which enables systems for patient monitoring. He men-

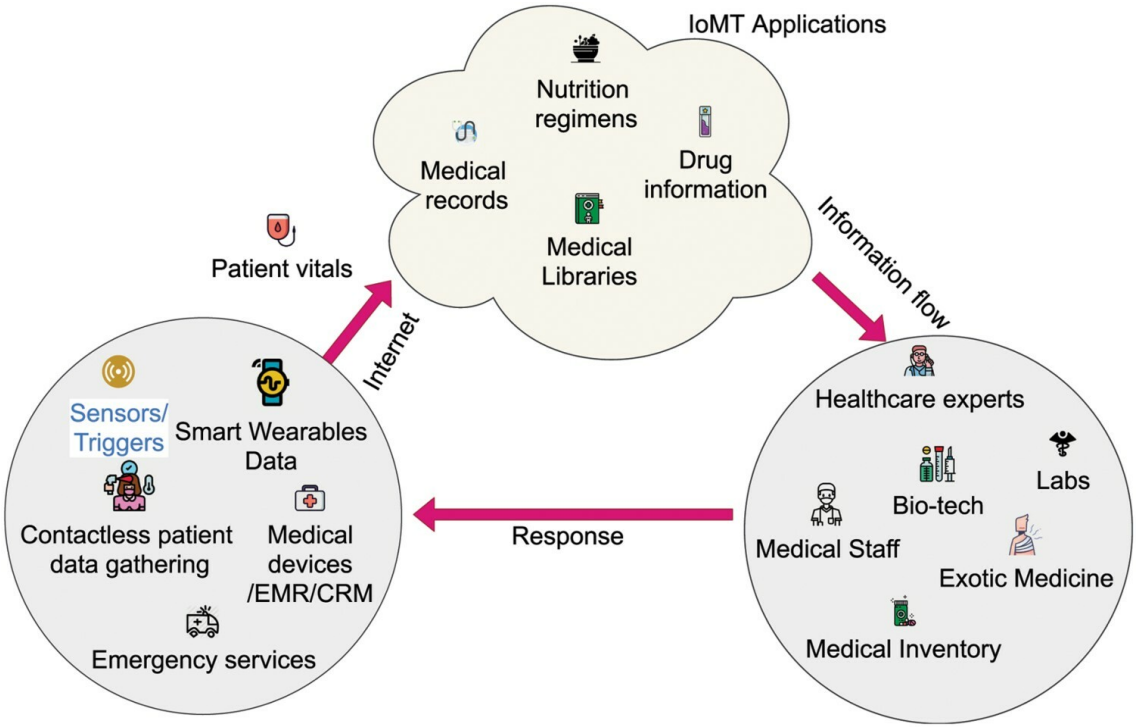

Figure 2.1: Information Flow in IoMT

tions that the cloud layer in the IoMT architecture acts as a central hub for data storage, computation, connectivity, and security. It enables efficient data processing, remote access to healthcare services, and scalability to accommodate the growing needs of the healthcare ecosystem. Considering the importance of the cloud layer, the present thesis work proposes an architecture focusing on the cloud layer.

2.2 Remote Patient Monitoring (RPM)

IoMT provides the underlying technological infrastructure and connectivity to enable remote patient monitoring and care delivery. Real-time patient data collection and transmission to healthcare providers via a variety of medical equipment, sensors, and communication systems is known as remote patient monitoring (RPM). This makes it possible for medical personnel to remotely check on patients' vital signs, symptoms, and other pertinent data. RPM allows healthcare professionals to keep

an eye on patients when they're not in traditional clinical settings—such as at home or in other remote places. Real-time or planned data collection and transmission of patient information to healthcare practitioners is accomplished by RPM through the use of a variety of IoMT devices, sensors, and digital communication tools. IoMT devices are essential to RPM since they can monitor a patient's health indicators continuously or sporadically and securely send the data to platforms for healthcare practitioners to monitor.

Activity trackers, blood pressure monitors, glucose monitors, and other medical sensors are examples of personalized healthcare wearables that are used in this system. These devices are linked to a central monitoring system. The patient data of these devices is routinely gathered and then sent via secure communication channels to healthcare providers. RPM helps identify changes in patient health status early on, facilitating prompt intervention and treatment. RPM Reduces healthcare expenses by reducing avoidable hospitalizations and the number of re-admissions. The high-level RPM architecture mentioned in the NCCOE publication named - "SECURING TELEHEALTH REMOTE PATIENT MONITORING ECOSYSTEM" [5] is considered as a reference and displayed in Figure 2.2.

This thesis focuses on secure data transfer in RPM in addition to interoperability and efficiency.

2.2.1 Use Cases of Remote Patient Monitoring

Remote patient monitoring has a wide range of use cases across various healthcare settings. One of the critical use cases of RPM is in the care of diabetic individuals. Diabetic patients track multiple metrics on a daily basis to lower long-term risks of problems and to improve self-control of their diabetes. These parameters are easily obtained using Remote Patient Monitoring, including blood pressure, blood glucose level, insulin consumption, weight, food, exercise and physical activity, and so forth.

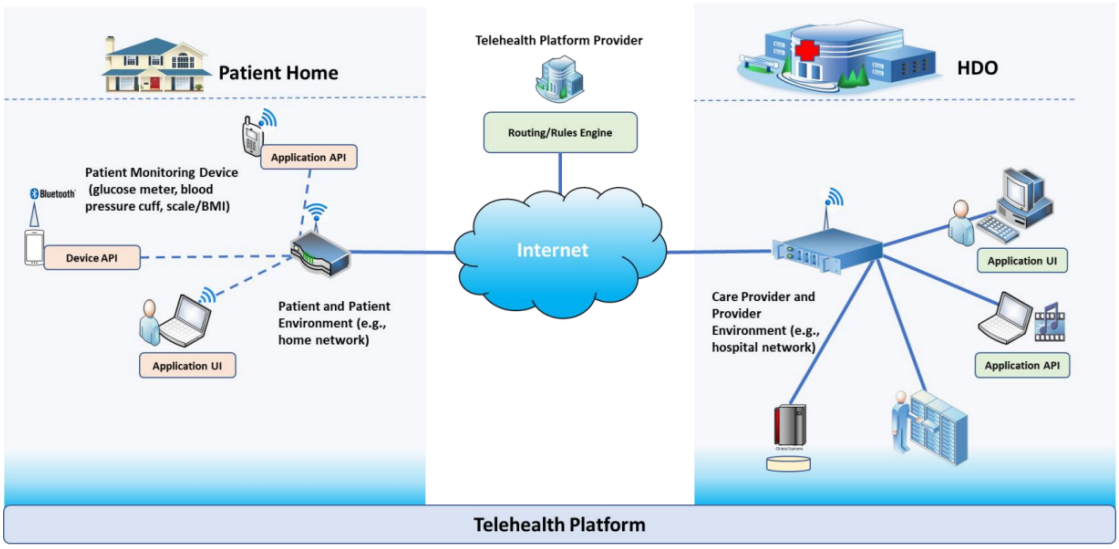

Figure 2.2: RPM architecture by NCCOE
Source: NCCOE NIST [5]

As mentioned by Zulj et al.[6], approximately half of adult diabetics go undiagnosed. Diabetes and its complications result in direct medical costs, lost productivity, and pay loss, which have a significant negative financial impact on health systems and national economies.

The following use case is to monitor heart health. Older persons require more frequent health examinations, increasing the pressure on current medical systems. In respected medical facilities, ECGs are often detected using stationary equipment. Frequent hospital visits can put a strain on healthcare systems. Remote monitoring of ECG signals can greatly assist in overcoming these obstacles. ECG monitoring systems can use a non-intrusive sensor to detect ECG signals, and they can use wireless transmission methods like Bluetooth or Zigbee to send the signal to a smartphone [7].

An interesting survey was made by Daly et al. [8] regarding the worthiness of the Remote Patient Monitoring System in view of Cancer patients. According to their survey, there was an 85% net promoter score. The majority of patients concurred

that the RPM was beneficial, improved their ability to control their COVID-19 symptoms, increased their sense of closeness to their medical team, and reduced the need for Emergency visits. In their literature, a National Comprehensive Cancer Center's COVID-19 RPM patients' viewpoints and levels of satisfaction were discussed. Hence, monitoring cancer patients is also one of the use cases.

In addition to the above-mentioned use cases, another application of RPM is pregnancy care, which includes pre-natal and post-natal care. Pregnant women can track fetal movements, blood pressure, and weight gain remotely, while healthcare providers monitor maternal and fetal well-being and intervene if necessary.

The most critical care group is the elderly patient. Older adults often have complex healthcare needs and may benefit from regular monitoring of vital signs, mobility, and medication adherence. RPM enables caregivers to monitor the health status of elderly patients remotely, detect changes in condition early, and coordinate care more effectively. The latest statistical updates from the United Nations mentioned that the elderly population is forecasted to be 2.1 billion in 2050 [9]. It is expected that more than 50% of the medical resources can be consumed by elderly patients resulting in a scarcity of medical resources. RPM is looked upon as the solution to manage this scarcity and provide on-time medical services to elderly patients. Aging people tend to forget their own health problems and/or are unable to visit the hospitals often. This will lead to numerous genuine restorative issues. Hence, the remote patient monitoring system with a human digital twin can help patients of such age overcome these challenges.

The proposed architecture considers these serious medical issues of elderly patients by integrating Azure IoT Hub with Azure Digital Twin to monitor the patients and predict based on the Human Digital Twin of such patients. The older population needs more care since their age-related physical changes, severe memory loss, and increased risk of falling are all greater than in younger adults [10]. The elderly

have greater needs for a wide range of medical services, particularly for family and community healthcare, as Figure 2.3 illustrates.

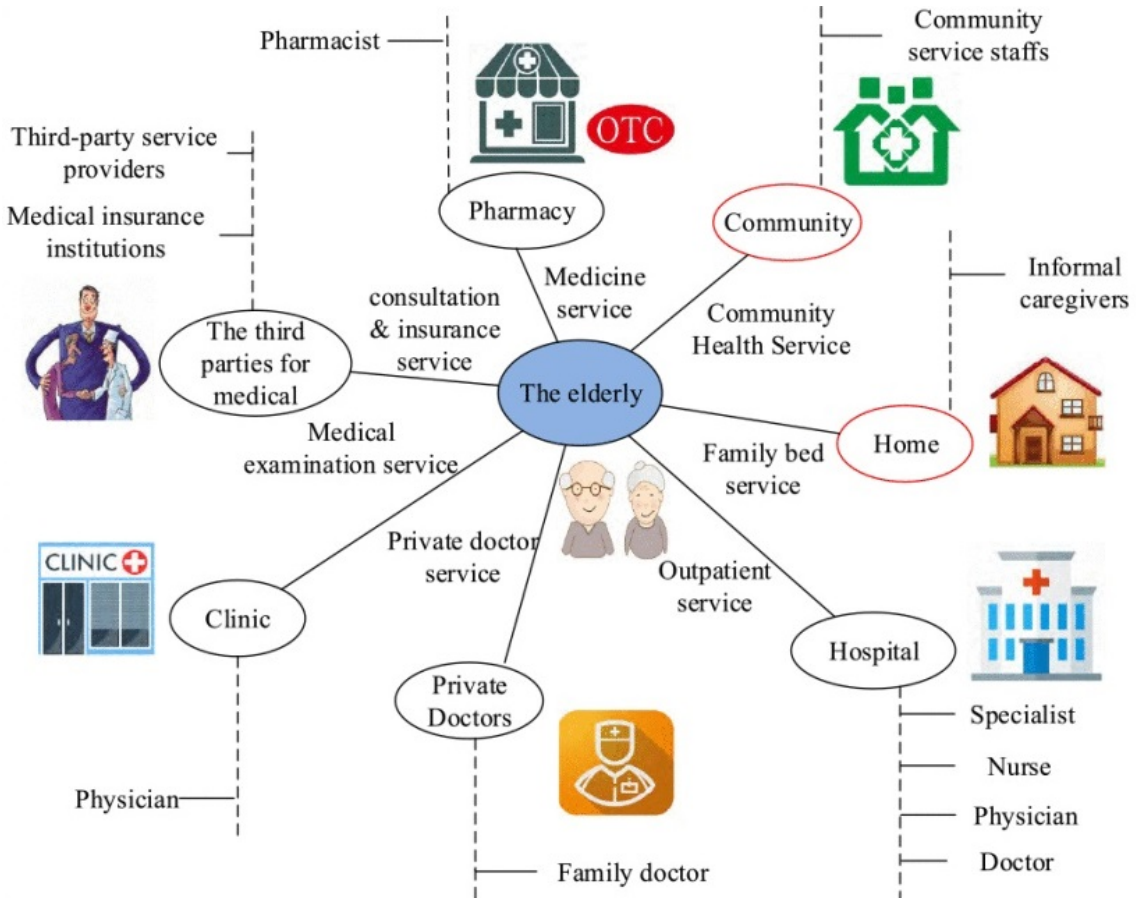

Figure 2.3: Healthcare Needs of Elderly Patients [10]

It is very vital to make sure that the data of patients in all the mentioned use cases are secure, whether the data is in motion or static. The attempt in the current proposed architecture is to make sure that Data privacy and security are given priority.

2.2.2 Security Threats in Remote Patient Monitoring

Numerous advantages of remote patient monitoring (RPM) for healthcare include better patient care, easier access to services, and lower medical expenses. Never-

theless, it also presents a number of security risks that must be resolved in order to protect patient confidentiality and data integrity. The following are a few typical security risks in remote patient monitoring:

1. **Data Privacy Issues:** Sensitive patient health information is transmitted and stored during RPM. Unauthorized access to sensitive information may result in identity theft, privacy violations, or other nefarious behaviour.

2. **Unauthorized Access:** To steal patient information, alter medical records, or interfere with healthcare services, hackers may try to get unauthorized access to remote monitoring systems.

3. **Data Interception:** There is a chance that hostile actors will intercept data being transmitted between medical devices and monitoring systems. The integrity and confidentiality of patient data may be jeopardized by this interception.

4. **Device Tampering:** It is possible to physically tamper with remote monitoring equipment, which might result in erroneous data gathering or altered device performance. The integrity of the data and patient safety may be at risk due to this tampering.

5. **Malware and Ransomware:** Healthcare systems, including remote monitoring platforms, are susceptible to malware and ransomware attacks. Malicious software can infect devices or networks, leading to data breaches, device malfunctions, or system downtime.

6. **Insider Threats:** Workers or anybody with permission to access remote monitoring systems may abuse their rights to see, alter, or reveal patient information for nefarious or personal gain.

7. **Denial-of-Service (DoS) Attacks:** To interrupt services, attackers may target remote monitoring systems. This could lead to patient care delays or jeopardize the availability of vital healthcare resources.

8. **Insecure Communication Techniques:** Patient data in remote monitoring

systems may be intercepted or accessed by unauthorized parties due to inadequate encryption techniques or insecure communication routes.

9. **Device Vulnerabilities:** Attackers may use software or hardware flaws in remote monitoring devices to take control of the equipment remotely or obtain sensitive patient data.

10. **Regulatory Compliance Issues:** Failure to comply with healthcare regulations and standards, such as the Health Insurance Portability and Accountability Act (HIPAA), may result in legal consequences as well as reputational loss.

To moderate these security dangers, healthcare suppliers and organizations ought to actualize strong cybersecurity measures, including encryption, access controls, standard security evaluations, staff education, and compliance with administrative necessities. Additionally, ongoing monitoring and proactive threat intelligence can help identify and address emerging security risks in remote patient monitoring systems.

2.2.3 Healthcare Cybersecurity Incidents

The Vastaamo data breach is a pivotal incident in Finland's cybersecurity history, involving unauthorized access and theft of sensitive patient information from a private psychotherapy service. The breach was publicly reported on October 21, 2020, but the hacking took place in two stages between November 2018 and March 2019. Vastaamo was a private psychotherapy service provider in Finland that operated multiple therapy locations nationwide. Personal information of approximately 36,000 patients containing names, residences, email addresses, social security numbers, and sensitive therapy session notes was accessed [11]. The incident prompted significant concern and anxiety among victims, sparking a national debate about mental health privacy and the value of data protection in healthcare. Many patients felt insecure as a result of the disclosure of their confidential therapy records. Following the hack

and the accompanying consequences, Vastaamo declared bankruptcy in February 2021 and moved its services to Verve. It served as a wake-up call for both private and public healthcare providers to enhance their data protection practices to prevent similar breaches in the future.

Another notable cyber attack in healthcare was Newfoundland and Labrador Healthcare Cyberattack. On October 30, 2021, a ransomware attack by the Hive ransomware organization significantly damaged Newfoundland and Labrador's hospital IT infrastructure. The hack caused widespread IT disruptions, requiring healthcare providers to use pen-and-paper methods for patient administration. The hack exposed personal and health information for the great majority of the province's inhabitants. By December 2021, most services had been restored, but the inquiry into the attack was ongoing [12].

A ransomware attack struck Medibank in late 2022, resulting in the theft of personal information from 9.7 million users, including sensitive medical records. The attack was carried out by a Russian cyber outfit [13]. A cyber incident at HCA Healthcare is also worth a mention. In July 2023, HCA Healthcare suffered a data breach that affected more than 11 million patients. The breach was traced back to a storage vulnerability in a third-party vendor, which exposed sensitive personal information such as names and birth dates [14].

Over the last five years, healthcare has seen a significant increase in cyberattacks, with an estimated 50% of healthcare organizations reporting at least one attack annually. According to the U.S. Department of Health and Human Services, there were over 1,500 reported healthcare data breaches affecting 500 or more individuals from 2018 to 2023. An estimated 40 million patient records were compromised in healthcare-related cyber incidents in the last five years. The average cost of a data breach in healthcare is approximately $9.23 million, significantly higher than other industries. Ransomware attacks in healthcare have increased by 150% from 2020 to

2023, with many organizations reporting operational disruptions lasting weeks.

From January 2021 to March 2023, the European Union Agency for Cybersecurity (ENISA) reported 215 publicly reported cyber incidents in the EU, with 208 specifically targeting the health sector. Basic web application assaults, system intrusions, and other failures accounted for 76% of cybersecurity breaches in the healthcare sector. Internal threat actors were responsible for 39% of these breaches. The COVID-19 epidemic resulted in a fivefold surge in cybercrime, as healthcare firms struggled to adapt to new digital settings, frequently ignoring cybersecurity safeguards [15].

Cybercrimes increased fivefold after the COVID-19 outbreak as healthcare businesses failed to adopt new digital environments and frequently neglected cybersecurity safeguards. The increasing frequency and severity of cyberattacks in the healthcare sector underscore the urgent need for robust cybersecurity measures. These breaches not only jeopardize patient privacy but also erode public trust in healthcare providers. The potential ramifications of cyber threats become more apparent as healthcare organizations depend more and more on digital technologies for patient care and data management. Therefore, implementing comprehensive cybersecurity strategies, including regular risk assessments, employee training, and advanced threat detection systems, is essential to safeguard patient information and ensure the continuity of care in an increasingly digital landscape.

2.3 Digital Twin in Healthcare

Michael Grieves then created the term "digital twin" (DT) in the context of product lifecycle management in 2005. The DT was used by NASA in 2010 [16], and by John Vickers [17] in 2012 as a virtual representation of a physical system.

A digital twin (DT) is a computerized model that accurately replicates a genuine object. A physical entity has been equipped with several sensors related to

important functional domains. These sensors generate data on many aspects of the physical object's functionality. After obtaining this information, the processing system actively combines it into a digital copy. Once the appropriate data is provided, the digital model can be used to run various simulations, investigate performance concerns, and propose potential changes. Obtaining valuable data that can be utilized to improve the original physical thing is the ultimate objective. Zheng et al. [18] defines a Digital Twin as a collection of virtual data that completely characterizes a possible or actual physical output from the microatomic level to the macro-geometrical level. Moreover, the definition by Barricelli et al. [19] defines the Digital Twin as a virtual model/representation that is linked to and continuously synchronized with a physical entity, allowing monitoring, control, optimization, and prediction of the physical twin's status and behavior.

DT-based healthcare research centers have been formed with the ultimate goal of improving patient care and tailoring wellness, disease preventive strategies, diagnosis, prognosis, and treatment. These centers aim to expand and improve the scope of DT technology and applications [20]. In healthcare, a DT should be individualized, interconnected, interactive, informative, and impactful (5Is) as scripted by Katsoulakis et al. [20]. Digital twins greatly improve patient care by utilizing advanced analytics and real-time data integration. They give medical specialists a comprehensive understanding of the patient, enabling them to design individualized treatment regimens. This method takes into account the unique traits of each patient as well as their medical background, genetics, and current physiological data. Consequently, therapies and drugs are customized to the patient's requirements, improving treatment results and patient satisfaction [21].

2.4 Human Digital Twin (HDT)

A human digital twin (HDT) is an online digital twin that is a virtual representation of a real person in the real world. Three elements are integrated into one digital representation of the patient (PT), virtual twin (VT), and medical records. While Digital Twin focuses on the partial functions of human organs and/ or medical devices, HDT focuses on the virtual twin of a complete human being. The simulated data and additional pertinent information gathered from the patient via wearable technology, sensors, and electronic health records serve as the foundation for the framework that is presented in this work. No matter where the patient is, the HDT allows for constant real-time monitoring of their vital signs, symptoms, and general health state. The HDT can offer tailored suggestions for medication adherence, lifestyle changes, therapy adjustments, and other interventions to enhance health outcomes based on the unique facts and features of each patient. The HDT is a technology that healthcare professionals can use for remote consultations. This eliminates the need for in-person sessions and gives them the ability to evaluate the patient's condition, make decisions, and offer direction.

Typical elements of the Human Digital in Remote Patient Monitoring can be represented as shown in Figure 2.4

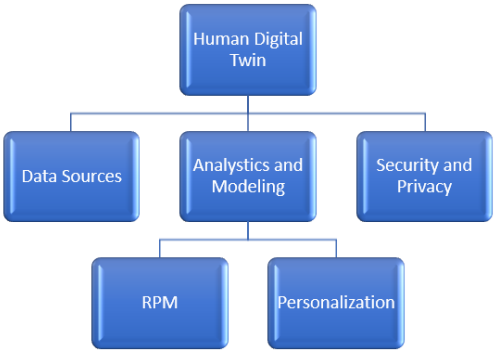

Figure 2.4: Elements of Human Digital Twin

Barricelli et al.[22] highlight that HDTs are customized computer representations

of people and are utilized in the medical field to track patients' health and deliver individualized therapy. Human-computer hybrid models, or HDTs, are customized computer representations of people that let medical professionals and researchers track their health and prescribe treatment plans. Conversely, DTs are virtual representations of physical systems that are employed to maximize efficiency and initiate self-healing and self-optimization processes. Whereas DTs are always linked and synced with their physical twins, HDTs are not in constant communication with them. In the medical and healthcare industries, HDTs are used to track patients' health and deliver individualized care. DTs are used to forecast problems and optimize performance in a variety of industries, including manufacturing and aviation.

2.5 OPC UA Standards

OPC UA (Open Platform Communications Unified Architecture) is a popular industrial communication standard noted for its reliability, security, and compatibility. OPC UA is also referred to as a standardized communication protocol that enables interoperability and data exchange between various devices, machines, and software applications. OPC UA provides a platform-independent, secure, and scalable framework for communication, data modeling, and information integration. In the context of the proposed architecture for remote patient monitoring (RPM), OPC UA facilitates seamless communication between various components such as healthcare devices, edge servers, Digital Twins, and other systems. OPC UA has strong security features like encryption, authentication, and access control, adhering to the CIA (Confidentiality, Integrity, and Availability) triad. OPC UA supports scalable communication architectures, allowing the RPM ecosystem to accommodate a large number of devices, Digital Twins, and users.

OPC UA does not depend on just one programming language or operating system (OS). It is based on Service-oriented (SOA) architecture and is robust in terms of

safety. OPC UA Information Model can be explained through the layer diagram shown in Figure 2.5

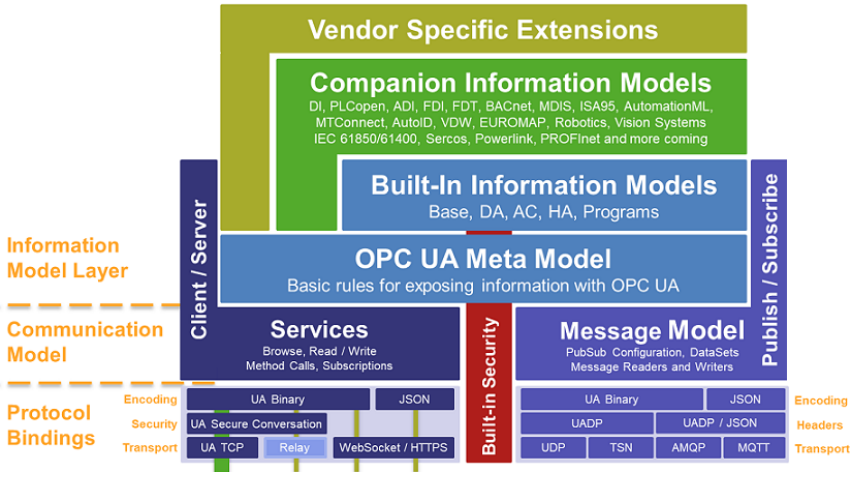

Figure 2.5: OPC Unified Architecture Overview.
Source: https://tinyurl.com/4swm6sjh

OPC UA adheres to international standards and industry best practices, making it well-suited for healthcare applications subject to regulatory compliance, such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). This compliance is crucial for safeguarding patient privacy and data security in remote monitoring.

2.5.1 OPC UA Architecture

The OPC UA architecture outlines a tiered approach with distinct security obligations assigned to each layer [23]. The IEC 62541 defines the OPC Unified Architecture or OPC UA. The Reference Architecture Model for Industries 4.0 recommends this platform-independent, service-oriented design. The defining of security elements for client-server communication was one of the main objectives of OPC UA [24]. It is important to mention that maximum of the other protocols focus on the Network layer, but the proposed model focuses on the Communication Layer. OPC UA offers a high degree of fundamental security features, including app authentication, user

authentication, confidentiality, integrity, and user authorization [24].

2.5.2 Security in OPC UA

Security in OPC UA is a critical aspect due to the sensitive nature of the data being transmitted. The three fundamental security levels of OPC UA are application, communication, and transport. A Defense-In-Depth strategy is achieved by each layer supporting its unique security features [24]. It supports various authentication methods, including username/password authentication, X.509 certificates, and integrated Windows authentication. Once authenticated, OPC UA allows administrators to define access control policies to regulate which users or client applications can access specific resources within the system. OPC UA uses cryptographic techniques like digital signatures and message digests to assure data integrity between clients and servers. OPC UA encrypts data to provide confidentiality over insecure networks. OPC UA provides secure communication channels through industry-standard protocols like TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security).

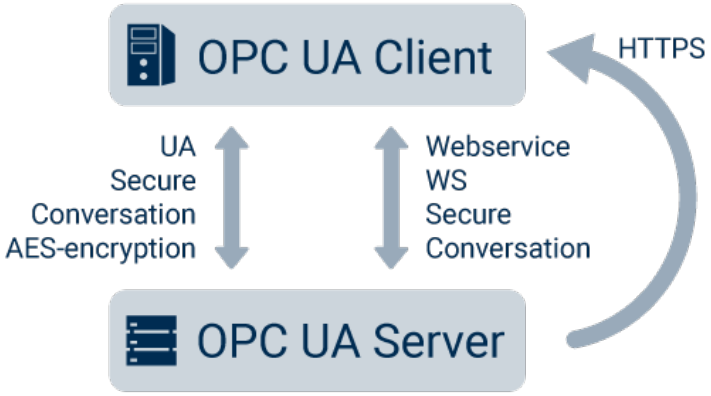

Figure 2.6: Security in OPC UA.
Source: https://www.opc-router.com/what-is-opc-ua/

2.5.3 Platform Independence and Interoperability in OPC UA

OPC UA defines a set of standardized communication protocols, including TCP/IP, HTTPS, and MQTT, which enable communication between OPC UA clients and servers across diverse network infrastructures. These protocols ensure that OPC UA-enabled devices and systems can communicate effectively, regardless of the underlying network technology. OPC UA provides language-neutral APIs (Application Programming Interfaces) and software development kits (SDKs) for implementing OPC UA clients and servers in various programming languages, such as C/C++, Java, .NET, Python, and JavaScript. These language-neutral APIs ensure that developers can create OPC UA applications using their preferred programming languages and development environments. OPC UA supports web services-based communication protocols, such as SOAP (Simple Object Access Protocol) and REST (Representational State Transfer), which enable integration with web-based applications and services. This integration facilitates interoperability between OPC UA-enabled industrial systems and web-based enterprise applications, IoT platforms, and cloud services.

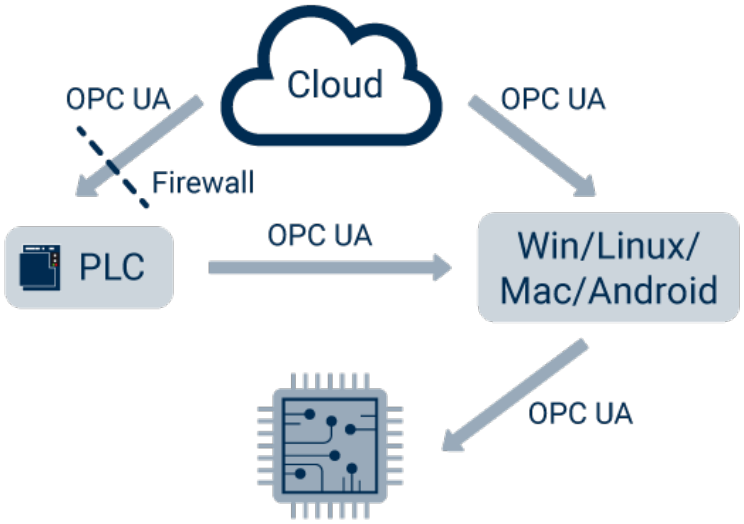

Figure 2.7: Platform Independence and Interoperability in OPC UA.
Source: https://www.opc-router.com/what-is-opc-ua/

2.6 Azure IoT Hub

IoT apps and the devices they monitor can communicate back and forth using Azure IoT Hub, a cloud-based service that serves as a central messaging hub. Azure IoT Hub offers a scalable and reliable platform that easily interacts with medical devices and data, which is a critical component in improving Remote Patient Monitoring (RPM) systems. Cloud real-time data from a variety of healthcare wearables and devices can be easily and securely ingested with Azure IoT Hub. This makes it possible for the Human Digital Twin to be updated continually with the patient's most recent health metrics, leading to more precise simulations and forecasts. Several data formats can be ingested by Azure IoT Hub, which can then normalize the data into a common format like FHIR (Fast Healthcare Interoperability Resources). The Fast Healthcare Interoperability Resources, or FHIR, is an interoperability standard for electronic health information exchange. Better analytics and insights are made possible by ensuring that the Human Digital Twin receives consistent, interoperable data from a variety of devices.

With the capacity to manage millions of devices and events per second, Azure IoT Hub is an incredibly dependable and scalable service. As a result, performance is not affected, and the Human Digital Twin can grow along with the number of patients and devices. End-to-end security is offered by Azure IoT Hub, which has capabilities that include encryption and per-device authentication. This protects private patient information entering the Human Digital Twin. Azure offers HIPAA compliance for workloads related to healthcare as well.

Azure IoT offers a reliable platform that makes intelligent and safe IoT solutions for the healthcare industry possible, thus improving patient outcomes. By providing a wide range of IoT services and health-specific app templates, it shortens the time to market for IoT solutions. Azure IoT, which is backed by multiple Azure Cloud components, guarantees the security of patient data from the edge to the cloud. Azure IoT Hub is a potent enabler for Human Digital Twins in remote patient monitoring due to its capacity to safely ingest, process, and scale real-time data from healthcare wearables. It helps medical practitioners to give patients better care by enabling the digital twin to operate as an up-to-date and accurate representation of their health.

IoT Hub enables medical devices to securely send telemetry data to the cloud and receive commands or updates from the RPM application. It also offers cloud-to-device and device-to-cloud messaging capabilities [25] [26]. Healthcare businesses can create scalable, compliant, and secure remote patient monitoring (RPM) systems that use Azure IoT Hub to identify health issues early and take appropriate action to improve patient outcomes and lower costs [26].

2.7 Related Work

Several studies have explored secure architectures for RPM. The main focus of the current research work is the Secure Remote Patient Monitoring System and safe,

personalized healthcare.

In the context of RPM, Majumdar et al. [27] has vividly discussed the importance and use of healthcare wearable sensors in Remote Patient Monitoring system. This article strongly supports the fact that wearable sensors play a critical role in remote health monitoring systems by providing continuous and non-invasive monitoring of physiological signs and activities, allowing for early detection and diagnosis of diseases, and improving the overall quality of healthcare for the elderly and those with limited access to healthcare facilities. As mentioned by Nora et al. [28], RPM enables continuous monitoring, diagnosis, prediction, and therapy. As a result, they cut healthcare costs and allow patients to go about their daily lives while constantly monitoring their vital signs.

Benedict [29] discussed the challenges of RPM related to managing the data transfers and connecting them using appropriate communication protocols. Fernandes et al. [30] proposed two different software frameworks IoT4Health and Agents4Health to perform the Remote Patient monitoring activities. These frameworks used Rest API to integrate IOT devices with the cloud. This article mainly focused on the analysis of the requirements of the Remote Patient Monitoring systems. Miranada et al. [31] proposed a conceptual architecture with heterogeneous networks for enabling Internet of Things (IoT) healthcare applications, using OPC UA as the communication stack. However, it is unclear how well the architecture can handle large-scale deployments and accommodate future growth and expansion of healthcare systems.

Saranya et al. [27], highlights the use of digital twin technology in healthcare can lead to benefits such as remote monitoring, group cooperation, analytical maintenance, transparency, future prediction, information sharing, big data analytics, cost-effectiveness, and improved patient care. Okegbile et al. [32] highly stress on the fact that HDT has the potential to revolutionize the existing healthcare system

by enabling personalized healthcare services (PHS). This article identifies and discusses the key technologies required for the development of HDT. In the context of personalized medicine, biomarkers are currently used in the provision of personalized medical care. Precision medicine requires new biomarkers to improve care for chronic illnesses like cardiovascular and neurodegenerative disorders. The rapidly emerging discipline of personalized or precision medicine is transforming clinical practice by focusing on the 'right patient - right treatment - right time' principle [33]. Biomarkers are integral to the advancement of personalized medicine, providing critical insights that enable tailored treatment strategies, improve diagnostic accuracy, and facilitate the development of targeted therapies. Their role in monitoring disease progression and treatment response further underscores their importance in achieving more effective and individualized healthcare solutions. However, Human Digital Twin (HDT) technology represents a significant advancement in personalized medicine compared to traditional biomarkers. While biomarkers have played a crucial role in understanding individual health profiles and guiding treatment decisions, HDTs offer a more comprehensive and dynamic approach to patient care.

Malasinghe et al. [34] provided the results of the survey related to major security challenges in RPM. These listed Data Confidentiality, Data Integrity, Data authentication, Data freshness, secure device-to-device communication, secure encryption, secure data storage, privacy protection and secure network communication between the remote monitoring system and the healthcare professional. In the interesting work by Boikanyo et al. [35], integration with existing healthcare systems is also one of the challenge in implementing Remote Patient monitoring. Getting patients and healthcare providers to accept and adopt RPM can be challenging. Greene et all. [36] presented the remote monitoring for the fall detection of patient. As per the paper, one of the main challenges in fall detection systems is finding the right balance between specificity and sensitivity.

As a solution to the challenges discussed in above mentioned scientific works, the current thesis proposes a comprehensive architecture to overcome most of them.

2.7.1 Literature Selection criteria

Peer-reviewed journal articles, conference proceedings, and books released within the previous ten years were all included. The search was conducted using scholarly resources such as Google Scholar, ScienceDirect, IEEE Xplore, and PubMed Central. White papers and industry reports from respectable organizations were also included. Keywords used to obtain the eligible articles are Secure protocols for Remote Patient Monitoring, Azure for Remote Patient Monitoring, Human Digital Twin for Secure Remote Patient Monitoring, and Integrate OPC UA with Azure Human Digital Twin.

2.7.2 Literature Analysis & Comparison

In order to improve security and privacy and ultimately provide safer and more individualized healthcare, the proposed research work is the first to investigate the integration of data from OPC UA-compatible healthcare wearable devices through Azure IoT Hub with Human Digital Twin in a Remote Patient Monitoring system. This thesis mentions a comparative analysis of various articles and research papers that are relevant to the topic of the study. By critically examining and synthesizing the existing literature, this thesis aims to identify key themes, gaps, and areas for further investigation. This review provides a solid foundation for the research and helps situate the study within the broader context of the field. These articles are drawn from reputable academic journals, conference proceedings, and other reliable sources. The selected articles cover a range of perspectives and methodologies, allowing for a comprehensive understanding of the topic.

Table 2.1 and Table 2.2 display the analysis of literature related to the research.

Author(s)	Focus Area	Key Contributions	Challenges/Issues Addressed
Miranda et al. [31]	OPC Unified Architecture (OPC UA) in healthcare systems	Proposed OPC UA for integrating heterogeneous healthcare systems; advantages of robustness, flexibility, compliance with Industry 4.0	Scalability, integration with existing systems
Benedict [29]	Communication protocols and security in RPM	Proposed OPC UA standard for secure data communication and device interoperability; addressed data security issues	Data theft, hacking, secure communication
Saranya et al. [37]	Digital Twin technology in healthcare	Benefits of digital twin technology: remote monitoring, transparency, predictive maintenance	Unauthorized access and manipulation of health data
Okegbile et al.[32]	Human Digital Twin (HDT) in healthcare	Emphasized personalized healthcare services, key technologies like Blockchain and AI	Privacy, security concerns, high latency in blockchain systems

Table 2.1: Comparison of Literature implementing OPC UA and HDT individually

In comparison to the existing work, this thesis proposes an architecture that combines the strengths of secure communication protocols, HDT technology, and advanced data analytics to provide a comprehensive framework for securing patient data and enhancing personalized healthcare in RPM systems.

To summarize, the literature study looks at the present status of research in remote patient monitoring, data security, tailored medication, and the use of Human Digital Twin technologies in healthcare. It emphasizes the expanding role of RPM in providing efficient and effective healthcare, particularly in chronic disease management and patient-centered care. The analysis goes into the vital importance of securing sensitive patient data in RPM systems in light of the growing danger of cyberattacks on telehealth technologies. The idea of personalized medicine is explored. Human Digital Twin technology is offered as a crucial approach to cus-

Author(s)	Focus Area	Key Contributions	Challenges/Issues Addressed
Majumdar et al. [27]	Healthcare wearable sensors in Remote Patient Monitoring (RPM)	Discussed cost-effective and real-time monitoring using wearable sensors for physiological signs; highlighted role in early detection and diagnosis, improving elderly care	Integration of wearable sensors, future use of Federated Learning
Nora et al. [28]	Importance of RPM	Emphasized continuous monitoring, diagnosis, prediction, therapy; improved quality of life; hospital prioritization based on illness	-
Fernandes et al. [30]	Software frameworks for RPM	Proposed IoT4Health and Agents4Health frameworks using REST API for integration with cloud	Lack of focus on data security and encryption
Malasinghe et al. [34]	Security challenges in RPM	Categorized security challenges: data confidentiality, integrity, authentication, encryption, secure communication	-
Meingast et al. [38]	Security concerns in health monitoring	Discussed data security, integrity, anonymity, regulatory compliance (HIPAA)	Privacy and security in distributed sensor networks
Boikanyo et al. [35]	Integration and acceptance of RPM in healthcare systems	Highlighted challenges of integration, reliable data transmission, and monitoring; emphasized the need for RPM in smart healthcare	Acceptance and adoption by patients and providers
Greene et al. [36]	Remote monitoring for fall detection	Focused on fall detection system challenges: balancing specificity and sensitivity	False negatives in fall detection, data sensitivity

Table 2.2: Comparison of Literatures

tomized healthcare, allowing for the production of virtual representations of patients that incorporate a variety of data sources. The literature research also looks into the use of secure communication protocols in healthcare systems, such as OPC Unified Architecture (OPC UA). It examines how OPC UA can promote interoperable and safe data sharing between medical devices and cloud platforms, which addresses the

requirement for standardized methods of data security.

3 Methodology

This section outlines the methodology adopted for developing the state-of-the-art framework and the components of the propose architecture for Next-Generation Patient Care, leveraging Human Digital Twin technology for personalized healthcare and security in remote patient monitoring (RPM). The architecture integrates healthcare wearable device data using OPC UA, employs pseudonymization for enhanced data security, and utilizes Azure IoT Hub and Azure Digital Twin for advanced analysis and prediction. The proposed architecture addresses key challenges in RPM systems and sets new standards in patient care through innovative technological integration and robust security measures.

3.1 State-of-the-Art Framework

The proposed architecture consists of innovative integration of secure communication protocols, advanced data pseudonymization techniques, and cutting-edge digital twin technology. It addresses key limitations of existing RPM systems by providing robust security, scalability, and real-time predictive analytics, thus setting a new benchmark for personalized healthcare solutions. The architecture diagram is proposed as in Figure 3.1. The proposed RPM is referred to as "SecureHealth" in the discussions throughout the thesis.

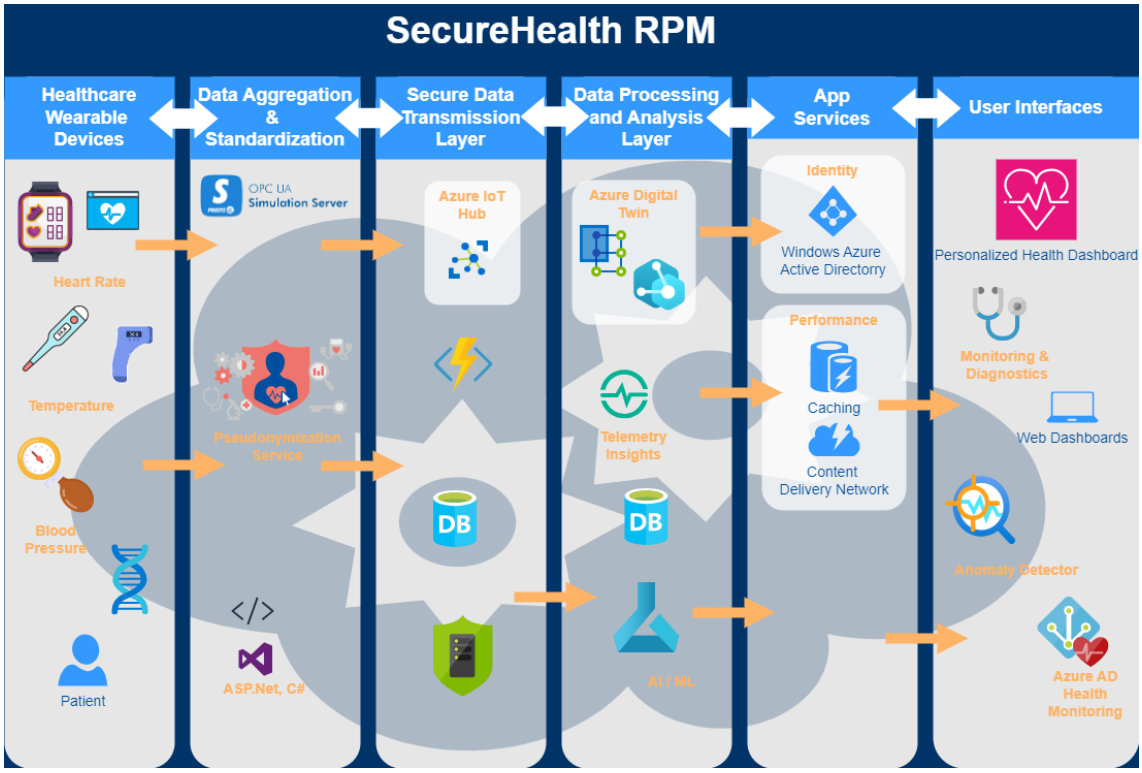

Figure 3.1: Proposed Architecture - SecureHealth RPM

3.1.1 Research Design

The study uses a mixed-methodologies strategy that includes both quantitative and qualitative methods. The quantitative component involves the comparison of the proposed SecureHealth RPM with existing RPM systems using the Chi-Square test. The qualitative component involves a detailed analysis of the proposed architecture's features and its alignment with state-of-the-art healthcare technology.

High-level architecture for the SecureHealth Remote Patient Monitoring represents the data flow from Healthcare Wearable Devices to OPC UA. These healthcare devices include invasive as well as non-invasive. At the core of the SecureHealth RPM is the OPC UA server, which serves as the gateway for data exchange between medical devices and the cloud platform. Patient data is pseudonymized to protect privacy while maintaining data utility for analysis and prediction. One of the com-

ponents of SecureHealth RPM is, the custom OPC UA client application developed using OPC UA client libraries and SDKs (Software Development Kits) to connect to OPC UA servers and communicate with Azure IoT Hub.

Further, the data from Azure IoT Hub is mapped to Azure Digital Twin using DTDL. When the value of property in the Human Digital Twin (HDT) changes, an email notification is sent to the Healthcare Provider to take necessary action. Three Azure IoT Hub devices are created to monitor the temperature, blood pressure, and heart rate of the patient. Each device is encrypted and has its own client ID and client secrets. Human Digital Twin has its own unique ID and credentials.

In the SecureHealth RPM System, the Prosys OPC UA server is considered to integrate the healthcare wearable device data into Azure IoT Hub through the OPC UA Client Application. This connectivity can be explained in Figure 3.2. Once the OPC UA client application retrieves data from OPC UA servers, it can publish the data to Azure IoT Hub for further processing and send to Azure Digital Twin. The client application formats the data into telemetry messages compatible with Azure IoT Hub's messaging protocols and sends them to Azure IoT Hub endpoints using the Azure IoT Hub SDK or client libraries. Telemetry messages may include metadata, timestamps, and additional context information to enrich the data sent to Azure IoT Hub. This cloud service acts as the central message hub, securely receiving data from wearable devices through OPC UA. Azure IoT Hub ensures reliable and scalable data ingestion, managing millions of device-to-cloud messages. The pseudonymized data is transferred to Azure Digital Twin for advanced analysis and prediction. Azure Digital Twin creates a virtual model of the physical entities, enabling detailed monitoring and simulation of patient health states.

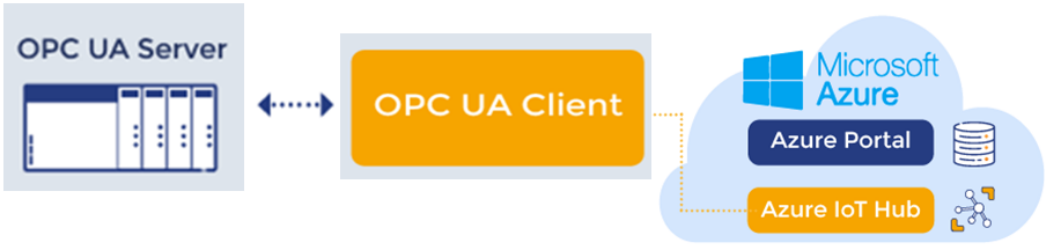

Figure 3.2: OPC UA to Azure IoT Hub

3.2 Evaluation of SecureHealth RPM System

This section evaluates the proposed architecture in comparison to the existing RPM systems as discussed in section 2.8.

In the proposed SecureHealth RPM system, by incorporating OPC UA, the interoperability and security challenges identified by Benedict [29] and Miranda et al.[31] are addressed. OPC UA provides a secure communication channel, reducing the risk of data breaches highlighted by Malasinghe et al.[34] and Meingast et al.[38]. The pseudonymization technique significantly enhances privacy by removing personally identifiable information from the data, addressing concerns raised by Saranya et al.[37] and Meingast et al.[38] regarding data privacy. OPC UA Standardization facilitates seamless integration of diverse wearable devices, addressing challenges mentioned by Fernandes et al.[30] regarding device integration. Azure IoT Hub efficiently handles data ingestion from wearable devices, addressing data transfer challenges identified by Benedict and Boikanyo et al. [35]. Strong security features including data encryption, access controls, and intrusion detection are provided by Azure IoT Hub and Azure Digital Twin, which strengthen the overall security posture. Azure Digital Twin enables advanced analytics, predictive modeling, and personalized healthcare, going beyond the data collection and analysis

focus of many reviewed works. By creating a virtual representation of a patient, Azure Digital Twin can be used to develop personalized care plans, predict health outcomes, and optimize treatment strategies, aligning with the potential of HDT discussed by Okegbile et al.[32]. The human digital twin in the proposed architecture provides a comprehensive digital representation of the patient, including their physical, physiological, and behavioural characteristics. This holistic model enables more accurate and personalized healthcare interventions, as the digital twin can capture the nuances and complexities of an individual's health status. The human-digital twin allows for advanced predictive analytics and simulation capabilities, enabling healthcare professionals to simulate different treatment scenarios and optimize personalized care plans. By leveraging the digital twin's data and modelling capabilities, the system can generate personalized predictions and recommendations tailored to the individual patient's needs and preferences.

In the SecureHealth RPM system, the integration of wearable device data and the human digital twin enables continuous monitoring of the patient's health status and real-time adaptation of care plans. This allows for proactive interventions and timely adjustments to treatment, improving patient outcomes and reducing the risk of adverse events. The comprehensive patient data and predictive capabilities of the human digital twin can support personalized preventive care strategies, helping to identify and mitigate potential health risks before they manifest. This proactive approach to healthcare can lead to improved patient outcomes, reduced healthcare costs, and a more sustainable healthcare system.

SecureHealth directly addresses several shortcomings found in the reviewed literature. Combining OPC UA, pseudonymization, and Azure's security features, it provides a more robust security framework.

3.3 Comparative Analysis of Communication Protocols

In the proposed SecureHealth RPM system for Next-Generation Patient Care, the choice of the OPC Unified Architecture (OPC UA) as the communication protocol is a strategic decision driven by several key factors that make OPC UA superior to other available protocols. This section details the rationale behind selecting OPC UA and its advantages in the context of integrating healthcare wearable device data, ensuring secure data transfer, and enhancing interoperability and scalability. In the context of the proposed architecture for Next-Generation Patient Care, it is essential to understand why OPC UA is the optimal choice over other existing protocols such as LoRa, Zigbee, Bluetooth Low Energy (BLE), and MQTT.

Table 3.1 compares some of the relevant protocols for healthcare with the OPC UA considered in the proposed architecture.

Criteria	**OPC-UA**	**LoRa**	**Zigbee**	**MQTT**	**BLE**
Security	High	Moderate	Moderate	High	Moderate
Interoperability	High	Low	Moderate	High	Moderate
Scalability	High	High	Moderate	High	Low
Latency	Low	High	Moderate	Low	Low
Reliability	High	Moderate	Moderate	High	Moderate
Ease of Integration	Moderate	Low	Moderate	High	High
Cost	High	Low	Low	Low	Low

Table 3.1: Comparison of Protocols

The time required to transmit data from a healthcare wearable device to a monitoring application depends on various factors, including the communication protocol used, the distance between the device and the server, and the amount of data being transmitted.

In the case of a remote patient monitoring system that implements the OPC

UA protocol, the time required to transmit data can be relatively faster than other protocols due to its efficient data transfer mechanisms and low latency. OPC UA is a machine-to-machine communication protocol that outlines specifications for data mapping, accessibility, security, and other characteristics, ensuring standardization and compatibility of data from OPC-UA-enabled equipment.

On the other hand, a remote patient monitoring system that does not implement OPC UA protocol may use other communication protocols such as Bluetooth, Wi-Fi, Zigbee, or cellular networks for data transmission. The time required to transmit data using these protocols can vary significantly.

For instance, Bluetooth is a short-range wireless communication technology that can transmit data up to 10 meters. According to a study, Bluetooth Low Energy (BLE) can transmit data at a rate of 1 Mbps, enabling fast data transfer between devices [39]. However, the range of Bluetooth is limited, and it may not be suitable for remote patient monitoring applications that require long-range communication. BLE Offers encryption and authentication but may be susceptible to certain attacks like man-in-the-middle attacks. Security primarily focuses on point-to-point communication. Interoperability is restricted to BLE-compatible devices and lacks standardized integration with broader systems. It is scalable for personal area networks but not ideal for large-scale systems. Flexibility is limited to short-range applications.

Zigbee is another wireless communication technology that can transmit data over longer distances than Bluetooth. According to a study, Zigbee can transmit data at a rate of 250 kbps, enabling faster data transfer than Bluetooth [40]. However, Zigbee's data transfer rate is lower than OPC UA, and it may not be suitable for applications that require high-speed data transfer. Zigbee provides basic security measures but can be vulnerable to certain attacks. Security configurations can be complex and less robust compared to OPC UA. It has limited interoperability with

non-Zigbee devices, primarily used for simple, local networks.

Cellular networks are another option for remote patient monitoring applications that require long-range communication. According to a study, cellular networks can transmit data at a rate of 10 Mbps to 100 Mbps, enabling fast data transfer between devices. However, cellular networks may have higher latency than other communication protocols, leading to slower data transfer.

Therefore, the time required to transmit data from a healthcare wearable device to a monitoring application depends on the communication protocol used, the distance between the device and the server, and the amount of data being transmitted. OPC UA protocol can provide faster and more efficient data transfer than other protocols, making it a suitable option for remote patient monitoring applications.

In the context of remote patient monitoring, LoRaWAN might not provide the same degree of security features and standards as OPC UA with Azure IoT, despite being appropriate for some IoT applications. OPC UA with Azure IoT's strong security framework, compliance with regulations, and seamless integration capabilities make it a preferred choice for ensuring data security and privacy in healthcare settings [41]. OPC UA with Azure IoT provides end-to-end encryption, robust device authentication, fine-grained access control, secure communication channels, and identity management services, ensuring comprehensive security for remote patient monitoring systems. On the other hand, LoRaWAN provides encryption at the network layer, device authentication, and secure communication channels, making it suitable for secure data transmission between remote devices and network servers in low-power, long-range IoT deployments.

OPC UA is designed to facilitate seamless communication between heterogeneous systems. This is particularly crucial in healthcare environments where diverse devices and systems, ranging from wearable sensors to cloud-based analytical platforms, need to interact seamlessly. Healthcare systems must be scalable to ac-

commodate a growing number of devices and flexible to integrate new technologies. OPC UA excels in both these aspects. It is adaptable to various network configurations and can be deployed in both small-scale and large-scale environments. OPC UA ensures high reliability in data communication, which is critical for real-time patient monitoring systems. The protocol's robustness against network failures and its capability to provide reliable data transfer even in unstable network conditions make it ideal for healthcare environments. OPC UA leverages X.509 certificates to enhance security.

As an open standard, OPC UA is vendor-neutral, preventing vendor lock-in and promoting a competitive market with diverse options for healthcare providers. The extensive community and industry support for OPC UA ensures continuous improvements, updates, and comprehensive documentation, facilitating its adoption and integration. With the rapid advancement of technology, it is crucial to select protocols that are compatible with future developments. OPC UA is aligned with Industry 4.0 principles, ensuring that it remains relevant as healthcare systems evolve towards more automated and intelligent environments. Its design allows easy integration with emerging technologies such as IoT and AI, making it a forward-looking choice.

This strategic choice supports the overarching goal of delivering next-generation healthcare solutions that are both secure and scalable.

3.4 Security Features

This section describes the security features of each component in the proposed architecture. OPC UA is crucial because the data being transmitted is confidential, frequently containing information about process control, industrial activities, and equipment status. OPC UA supports secure communication channels using industry-standard protocols such as Transport Layer Security (TLS) and Datagram

Transport Layer Security (DTLS).These protocols protect the confidentiality, integrity, and authenticity of data sent between clients and servers by encrypting communication channels and requiring mutual authentication between participants. Pseudonymization is an extra security layer that complements the existing security capabilities of OPC UA and Microsoft Azure. This is implemented to encrypt the data transmitted from OPC UA server to the Azure IoT Hub. Additionally, each IoT Hub Device is encrypted with configured security mechanisms. Security mechanisms provided by Azure IoT Hub are Symmetric, X.509 Self Signed and X.509 CA Signed.

3.4.1 Pseudonymization

In Article 4(5) of the GDPR, pseudonymization is defined as, *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"* [42].

Pseudonymization and encryption are two methods of data protection. Still, pseudonymization has particular advantages in the context of healthcare settings because it replaces identifiable data with artificial identifiers or pseudonyms for personally identifiable information (PII), allows analysis and usefulness of data while protecting individual privacy. In contrast, encryption renders data unreadable without a decryption key, with limited capabilities restricting the use of that data for research and personal care. Pseudonymization preserves the capacity to re-identify people with the aid of supplementary data stored apart, such as a key or lookup table. This reduces the possibility of illegal access or exposure while preserving the usefulness of the data for processing and analysis. Data that has been pseudonymized can

be returned to its original form by adding details that enable the re-identification of the individuals. This technique ensures that while the data remains relevant for analysis, it is not easily traceable back to particular patients. The pseudonymization process complies with data protection regulations such as GDPR, ensuring that patient privacy is maintained throughout the data lifecycle. Without the associated pseudonymization key, an attacker would not be able to directly identify people even if they were to obtain pseudonymized material [43].

Pseudonymization is a vital privacy-enhancing strategy used in healthcare that helps institutions maintain a balance between the necessity of data analysis and sharing and the need to preserve patient privacy and adhere to legal obligations. Healthcare businesses can protect patient privacy rights and maximize the value of their data assets by pseudonymizing patient data. Patients' confidence in the security of their health information is increased, and compliance with data protection laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), is ensured.

Consider Alice, who has been diagnosed with a heart condition (CVD) and experiences episodes of atrial fibrillation, which can elevate her risk of a stroke. Pseudonymization in this case can be visualized in Figure 3.3.

Alice's wearable device continuously tracks her heart rate and whether she is moving. It can alert Alice if her resting heart rate drops below the Low threshold or exceeds the High threshold.

Instead of sharing Alice's exact heart rate figures and specifics, the wearable device uses pseudonymization. This means that when it sends data, it transmits a pseudonym for Alice along with the parameter range for her heart rate at rest. The healthcare providers, such as her physician, caregivers, or midwives, will receive this pseudonymized data. They will be able to identify which patient the pseudonym refers to and understand the state of Alice's heart rate at rest without directly

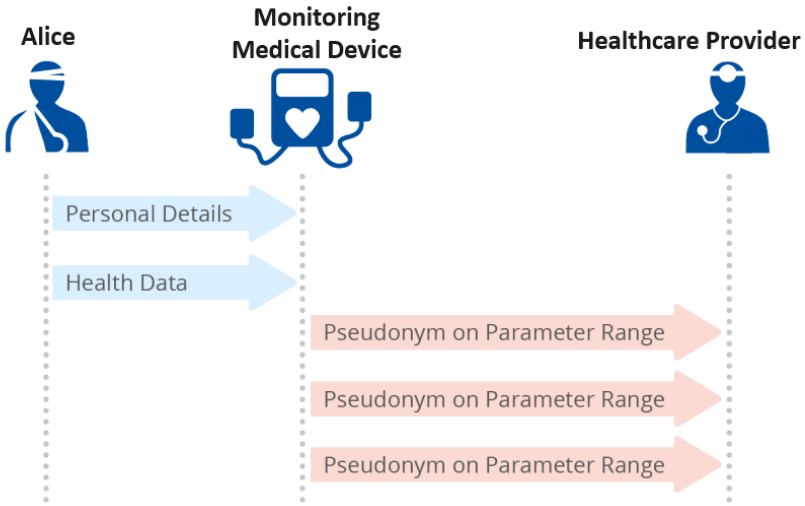

Figure 3.3: Pseudonymization during monitoring of health data

accessing her personal information.

When an alert is triggered, indicating that Alice's heart rate is outside the defined safe range, the pseudonymized data is sent securely to her physician and any designated caregivers or midwives. They receive a notification with the pseudonym and the specific heart rate range (e.g., Low or High). Since they have access to the pseudonymization key, they can identify Alice and provide the necessary support promptly. This process ensures that Alice's personal health data is kept confidential during transmission, enhancing security and privacy while allowing her healthcare team to respond effectively to her needs.

3.4.2 Azure Active Directory

The key security feature of Azure IoT Hub and Azure Digital Twin is the Azure Active Directory (Azure AD) integration for authentication and identity management. Each IoT Hub device has its own unique ID. The data ingestion from the OPC UA client application is mapped to only authenticated Azure IoT Devices. Similarly, the HUman Digital Twin created in Azure Digital Twin Explorer also has a unique I,D which can be mapped with IoT Hub device data. Only authenticated and au-

thorized devices are updated. Azure IoT Hub and Azure Digital Twin have built-in threat detection capabilities to identify suspicious activities and potential security breaches. There are continual backups and data replication to ensure data integrity and availability in the event of hardware failures or disasters. Device-to-cloud and cloud-to-device communication channels are encrypted to maintain the confidentiality and integrity of patient health data. Role-based access control (RBAC) allows administrators to control access to IoT Hub resources and data streams. Azure IoT Hub provides built-in monitoring and logging capabilities to track device connectivity, message ingestion, and system health.

3.4.3 Encryption of data at rest

Azure Digital Twins encrypts data as it is written in Microsoft data centers, both in transit and at rest, and then decrypts it when needed. A Microsoft-managed encryption key is used to perform this encryption. This feature is known as **Encryption of data at rest**. This feature helps to encrypt and decrypt data quickly. Encryption at rest provides protection to data that is stored i.e. at rest. A symmetric key encryption is used in this process. The data is encrypted and decrypted using the same key. However, if data is partitioned, then each partition has a unique key. Attempts to physically access the hardware that stores the data and subsequently compromise the data within are examples of attacks on data at rest. Encryption at rest prevents the attacker from accessing unencrypted data by ensuring that the data is encrypted while it is on disk. To read the data on a hard drive containing encrypted data but missing the encryption keys, an attacker must first break the encryption.

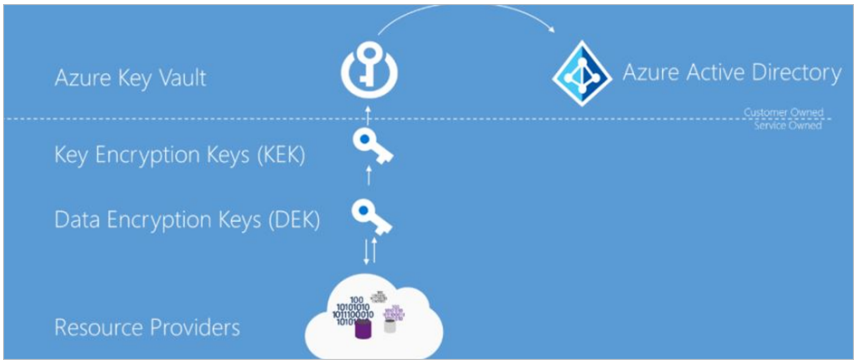

Figure 3.4: Azure Data Encryption-at-Rest Components
Source: [44]

3.5 Threat Analysis

This section outlines the possible threats in existing RPM systems, out of which one is the "IoT-based heart monitoring system" [45] and the second is the "A Real-Time Heart Monitoring System for Remote Cardiac Patients Using Smartphones and Wearable Sensors" [46]. The focus of the thesis is to analyze the existing RPM system for heart monitoring and how the proposed architecture can address the same.

Table 3.2 provides an overview of the possible data-related security threats to both the IoT-based heart monitoring system and the real-time heart monitoring system for remote cardiac patients, highlighting areas where each system may be vulnerable.

In addition to data-related threats, there are multiple existing threats. This can be listed in Table 3.3

Next section discusses about how SecureHealth can address most of the threats identified in both of the existing RPM systems discussed in this section.

Threat	IoT-based Heart Monitoring System	Real-time Heart Monitoring System
Data Interception	Interception of data during transmission despite 128-bit encryption	Interception of BLE transmissions
Data Integrity	Potential tampering of JSON files during transmission	Potential lack of integrity checks during storage on SD card
Data Theft	Theft of sensitive data through unauthorized access	Theft of patient data from the smartphone or during transmission
Data Loss	Loss of data due to transmission errors or device failures	Data loss due to failure of the smartphone or SD card
Privacy Breach	Unauthorized access to personal health information	Inadequate privacy measures for data stored on the smartphone
Encryption Weaknesses	Potential weaknesses in the 128-bit encryption implementation	Possible weaknesses in BLE encryption mechanisms
Replay Attacks	Replay of intercepted authentication tokens	Replay of intercepted BLE transmissions
Man-in-the-Middle (MitM) Attacks	MitM attacks during data transmission between devices and Firebase	MitM attacks during BLE communication or between smartphone and web portal

Table 3.2: Data Security Threats in existing RPM Systems

3.5.1 Addressing Threats in existing State-of-art

The proposed RPM architecture leverages a combination of security techniques, including pseudonymization, OPC UA, Azure IoT Hub, and Azure Digital Twin, to enhance the protection of patient data and enable personalized healthcare services. These security features help address the key concerns of data privacy, integrity, and access control in remote patient monitoring systems.

Addressing Threats in the IoT-based Heart Monitoring System [45]

Since the patient data in the proposed RPM architecture remains anonymous and impossible to relate to specific people, adopting pseudonymization helps reduce the dangers of unwanted access and data interception. Strong security features of OPC

Threat	IoT-based Heart Monitoring System	Real-time Heart Monitoring System
Unauthorized Access	Compromise of Firebase authentication tokens	Unauthorized access to patient data stored on the smartphone
Device Impersonation	Spoofing of device tokens	Spoofing of BLE devices
Denial of Service (DoS)	Flooding the system with invalid requests to disrupt service	Overloading the BLE connection or web interface to disrupt monitoring
Weak Authentication	Exploitation of weak or improperly implemented authentication	Compromise of user ID and password on the web interface
Malware	Introduction of malware through compromised devices or connections	Infection of the smartphone or web interface with malware
Insider Threats	Malicious actions by authorized users	Malicious actions by healthcare professionals with access to the web portal
Configuration Flaws	Misconfiguration of Firebase security rules	Misconfiguration of web interface or smartphone security settings
Firmware Exploits	Exploitation of vulnerabilities in the IoT device firmware	Exploitation of vulnerabilities in the wearable sensor firmware

Table 3.3: Security threats in existing RPM sytems

UA, like role-based access control and end-to-end encryption, guard against service account vulnerabilities and token misuse in addition to preventing unwanted access to wearable device data [47]. Azure IoT Hub's security features, such as encryption of messages and device authentication, offer an extra degree of security for data transmission to the cloud, mitigating possible risks found in the IoT-based cardiac monitoring system.

Addressing Threats in the Real-Time Heart Monitoring System [46]

The authentication and encryption features of OPC UA reduce the possibility of BLE data interception and eavesdropping by securing data transmission between wearables and the cloud [47]. Azure Digital Twin's secure data storage and access

control capabilities guarantee that patient data is shielded from unwanted access even in the event that a web portal or smartphone is attacked. The possible weaknesses in the web portal access restrictions are addressed by integrating the RPM architecture with Azure Active Directory for user authentication and permission. To detect and stop data tampering during transmission and storage, the RPM architecture can make use of data integrity checks, such as digital signatures or cryptographic hashing [48].

3.5.2 Summary of Security Threats addressed by the SecureHealth

This section discussed the security threats addressed by SecureHealth. The proposed architecture ensures the confidentiality, integrity, and availability of patient data, thereby enhancing the overall security and reliability of remote patient monitoring systems.

- Ransomware: The research found that by combining OPC UA with Azure IoT, healthcare organizations may establish secure communication channels, deploy encryption methods, and apply access control mechanisms to prevent ransomware attacks that could risk patient data. This is one of the important factors examined when proposing SecureHealth.

- Insider Threats: The authentication and authorization features in OPC UA to combat insider threats effectively. Azure IoT's monitoring capabilities further enhance the detection of suspicious activities, ensuring that only authorized personnel can access critical healthcare systems and patient information.

- Denial of Service (DoS) Attacks: Azure's scalable infrastructure can dynamically allocate resources and distribute incoming traffic across multiple servers,

mitigating the impact of DoS attacks by ensuring the availability and performance of OPC UA services. OPC UA implementations can implement rate limiting and request validation mechanisms to filter out malicious requests and mitigate the impact of DoS attacks on healthcare systems.

- Man-in-the-Middle (MitM) Attacks: OPC UA employs Transport Layer Security (TLS), which encrypts communication channels between devices and cloud servers. Azure's secure communication channels further enhance protection against MitM attacks by providing a secure platform for data transmission. Data is shielded from unauthorized parties via encryption, even if it is thwarted.

- Data Tampering: OPC UA ensures message integrity through digital signatures, which detect any alterations to the data during transmission. Azure's data integrity verification mechanisms further enhance protection against data tampering by ensuring that data remains unchanged while stored in the cloud. Additionally, access controls and audit trails help track changes to patient data, making it easier to detect and mitigate tampering attempts.

- Unsecured IoT Devices: The security challenges associated with healthcare IoT devices emphasize the critical need for secure communication protocols like OPC UA. By utilizing OPC UA with Azure IoT, organizations can ensure that IoT devices communicate securely and only with authorized systems, reducing the risk of unauthorized access and potential breaches

- Legacy Systems Vulnerabilities: The vulnerabilities identified in industrial control systems using OPC UA underscore the importance of bridging legacy systems with modern IoT platforms securely. OPC UA's ability to facilitate secure data transfer without compromising older systems' integrity, when combined with Azure IoT's advanced security features, helps mitigate risks

associated with legacy systems vulnerabilities.

- Secure Communication: OPC UA provides end-to-end encryption and authentication mechanisms to ensure data confidentiality and integrity.

- Access Control: Azure IoT's role-based access control combined with OPC UA's user authentication capabilities helps restrict unauthorized access to critical healthcare systems and patient data.

4 Framework Implementation

4.1 Data Collection and Preprocessing

Patient health data is the key data for proposed model of RPM. Required patient data include name, age, heart rate and temperature. As part of this research work, actual hardware devices are not connected.

4.1.1 Pseudonymization

Pseudonymization plays a crucial role in enhancing the privacy and security of patient data in the proposed SecureHealth RPM system. The pseudonyms are assigned to patient data collected by healthcare devices and integrated into the OPC UA Simulation Server. This ensures that sensitive patient information is not directly linked to identifiable individuals at the source. Pseudonymization can be implemented at each layer of the architecture, but the present work contributes to the analysis of implementation at the Data collection layer.

The specific data elements of the patient are identified within the available patient data that constitute personally identifiable information (PII). This includes Name, Age, BloodPressure and Temperature. There are multiple mechanisms to generate the pseudonyms. These techniques include the hashing process and/or salt addition. In the code provided in this work, the SHA-256 hashing algorithm is applied to each PII element individually. Then, it is converted into the hexadecimal

hash value.

4.2 Digital Twin Representation

Digital Twin representations of individual patients are created using DTDL, defining the structure and metadata of each Digital Twin. These Digital Twins encapsulate patient health data, historical information, and other relevant context, providing a holistic view of patient health status.

4.2.1 Human Digital Twin Creation in Microsoft Azure

Azure Digital Twins are for modelling and managing digital twins. Azure Digital Twin offers several benefits, including standardized modelling, interoperability, and scalability. In SecureHealth RPM system, a specific language known as the Digital Twin Definition Language (DTDL) is used to define DT.

4.3 Digital Twin Definition Language(DTDL)

DTDL provides a standardized way to describe the structure and behaviour of digital twins, enabling interoperability, integration, and communication between different IoT platforms, devices, and applications. DTDL provides a standardized language and schema for defining the attributes and characteristics of digital twins, including Human Digital Twins. This standardization ensures consistency and interoperability across different implementations and platforms. DTDL allows for flexible modelling of Human Digital Twins, enabling organizations to define custom properties, behaviours, and relationships that accurately represent individual users or groups of users.

In the proposed architecture, Azure Digital Twin Explorer is used to create the Human Digital Twin. Using DTDL within Azure Digital Twin Explorer helps main-

tain consistency in data modelling and representation. Azure Digital Twin Explorer integrates seamlessly with other Azure services and tools, such as Azure IoT Hub, Azure IoT Central, Azure Stream Analytics, and Azure Machine Learning. Azure Digital Twin Explorer supports role-based access control (RBAC) and Azure Active Directory (Azure AD) integration, enabling the definition of fine-grained access policies and control access to Human Digital Twins based on user roles and permissions [49]. This helps ensure that sensitive user data is protected and compliant with privacy regulations.

4.3.1 DTDL Specification Implementation

Data is a key in the Digital Twin. DTDL is compatible with JSON. The version of DTDL being used must be specified when developing a digital twin specification. Since DTDL is built on top of JSON-LD, the version of DTDL being used is specified via the JSON-LD context (the @context declaration). In the proposed architected DTDL v3 is used to create the Azure Digital Twin for a patient. We need to define the properties, telemetry, commands, and relationships of the human digital twin using DTDL. This includes attributes such as temperature and blood pressure as part of the current research work. All digital twins must have an identifier that is a digital twin model identifier (DTMI). It is required to specify metadata such as data types, units, and semantic meanings for each property. A simplified DTDL model for a Human Digital Twin is considered as part of this research work. A Digital Twin model's attributes, which are specified in the contents portion of the model interface, provide the majority of its information. A DTDL model interface used for Azure Digital Twins mainly contains fields like Property, Relationship and Component. Property describes the state as well as the synchronization of state between different IOT devices. The properties are defined as shown in Figure 4.1. They are the Name, Age, Heart Rate, and Temperature of a patient. This DTDL

model represents the Human Digital Twin for an elderly patient who needs to be monitored remotely.

```
{
  "@context": "dtmi:dtdl:context;2",
  "@id": "dtmi:com:example:HumanTwin;1",
  "@type": "Interface",
  "displayName": "Human Digital Twin",
  "contents": [
    {
      "@type": "Property",
      "name": "name",
      "schema": "string",
      "displayName": "Name"
    },
    {
      "@type": "Property",
      "name": "age",
      "schema": "integer",
      "displayName": "Age"
    },
    {
      "@type": "Property",
      "name": "heartRate",
      "schema": "double",
      "displayName": "Heart Rate (bpm)"
    },
    {
      "@type": "Property",
      "name": "temperature",
      "schema": "double",
      "displayName": "Temperature (°C)"
    }
    // Add more properties as needed
  ]
}
```

Figure 4.1: DTDL Code for HDT

In this model: - ‘name‘ is a string property representing the name of the person. - ‘age‘ is an integer property representing the age of the person. - ‘heartRate‘ is a double property representing the heart rate of the person in beats per minute (bpm).

- ‘temperature‘ is a double property representing the temperature of the person in degrees Celsius (°C).

The above DTDL model is created in Notepad and saved as a .json file, and then uploaded in the Azure Digital Twin Explorer, as shown in Figure 4.2.

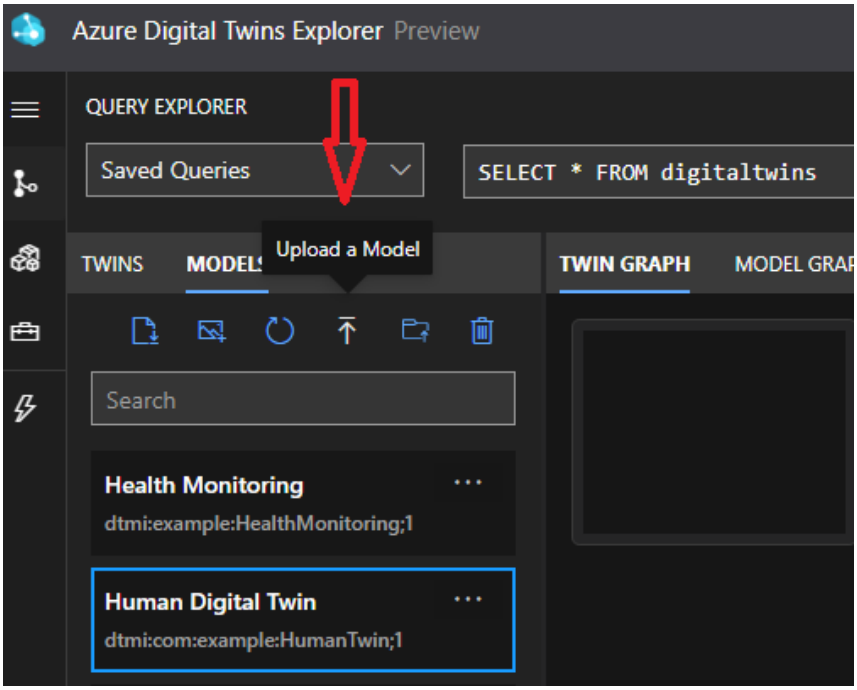

Figure 4.2: Uploading DTDL Json Model

4.4 OPC UA Integration

For the testing of the proposed architecture, a C#.Net application is created to integrate OPC UA (Open Platform Communications Unified Architecture) with Azure IoT Hub. The data from the Prosys Simulation server is read through the C# console application and transmitted to the Azure IoT Hub Device.

1. Install and configure an OPC UA server such as an OPC UA Simulation Server or Prosys OPC UA Simulation Server.

2. Configure the server to expose the necessary data points (nodes) that are to

be monitored or controlled. In the present work, the Heart rate, Temperature, and Blood Pressure of the patient are considered to be monitored.

3. Login to the Azure Portal and create a new Azure IoT Hub instance.
4. Get the connection string for the IoT Hub.
5. Install the Prosys OPC UA .NET SDK via NuGet Package Manager in the Visual Studio project.
6. Create a new .NET Console application in Visual Studio.
7. Use the Prosys OPC UA .NET SDK to implement OPC UA client functionality.
8. Establish a connection to the Prosys OPC UA Server using its endpoint URL.
9. Browse the server's address space to discover available nodes and select the nodes to monitor or control.
10. Implement logic to read data from OPC UA nodes and send it to Azure IoT Hub.
11. Use the Azure IoT Hub SDK for .NET to send telemetry messages and receive cloud-to-device commands.
12. In the .NET application, use the Azure IoT Hub connection string obtained earlier to connect to Azure IoT Hub.
13. After reading the data from the OPC UA simulation server, apply the Pseudonymization logic to this data so as to strongly encrypt the same.
14. Implement code to send pseudonymized data to Azure IoT Hub as telemetry messages and to receive commands from Azure IoT Hub.

15. Implement device authentication mechanisms provided by Azure IoT Hub by using a unique Device ID.

16. Next, integrate this pseudonymized data from Azure IoT Hub to Azure Digital Twins. Use the Azure IoT SDK to facilitate communication with the Azure IoT Hub.

4.5 Experimental Setup

The experimental setup includes Prosys OPC UA Simulation Server for data exchange and integration of Healthcare wearable devices, Visual Studio IDE for Data Simulation and integration with Azure Cloud services, and Azure Portal Configuration for data processing, security, and prototyping of the remote patient monitoring system.

The first step is to install and configure the Prosys OPC UA server which is free software available on request. Once the Prosys OPC UA Simulation server is installed, the configuration displayed is in Figure 4.3.

Figure 4.3: Prosys OPC UA Simulation Server

As part of this research work, the temperature and Heart Rate of the patient are monitored.

The node for Temperature is created in the Prosys OPC UA server as shown in Figure 4.4

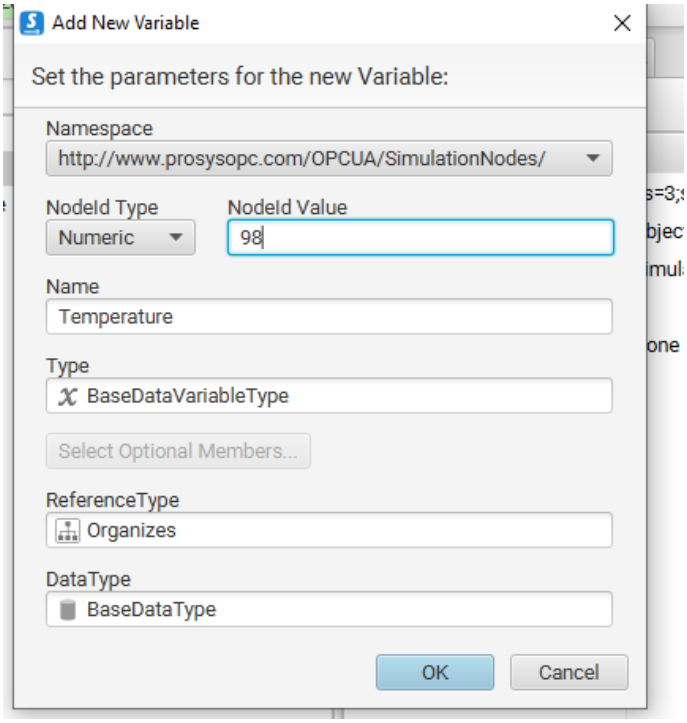

Figure 4.4: Temperature

A summary of the complete steps for data flow in the SecureHealth RPM is explained in the following section.

Step 1: Create Azure IoT Hub Instance. Figure 4.5 displays the Azure Dashboard after creating the Azure IoT Hub.

Step 2: Create IoT Hub devices that we want to integrate with OPC UA. IoT Hub devices are created to monitor the temperature, heart rate and blood pressure of the healthcare devices data integrated with OPC UA. Figure 4.6 displays the Azure Device Management dashboard.

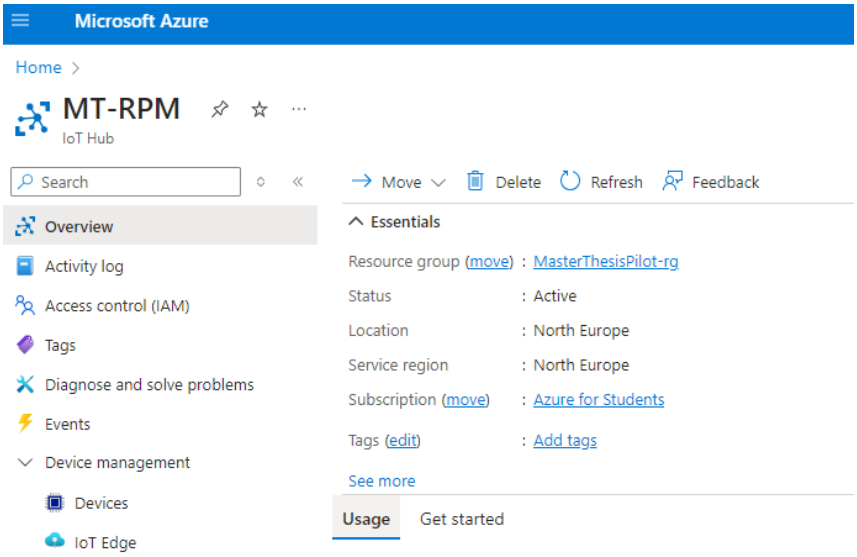

Figure 4.5: Azure IoT Hub Instance

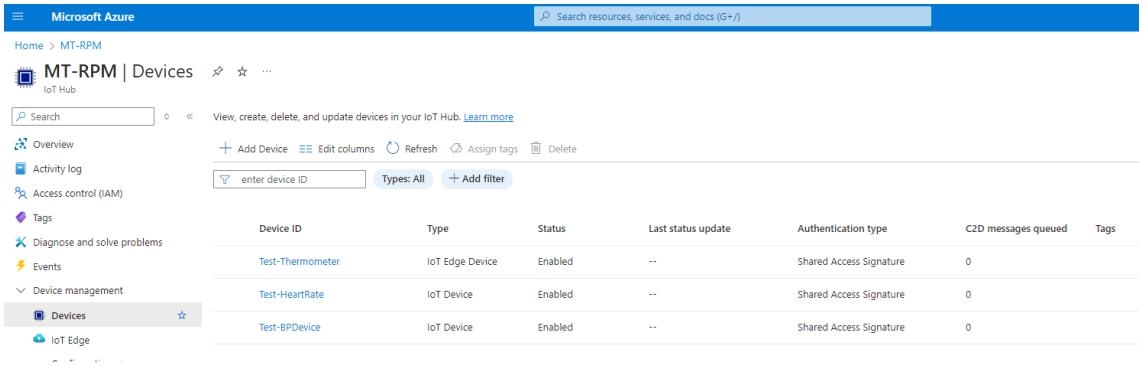

Figure 4.6: IoT Hub Device

Step 3: Create Human Digital Twin in Azure Digital Twin Explorer. Model Information can be seen in Figures 4.7 and 4.8

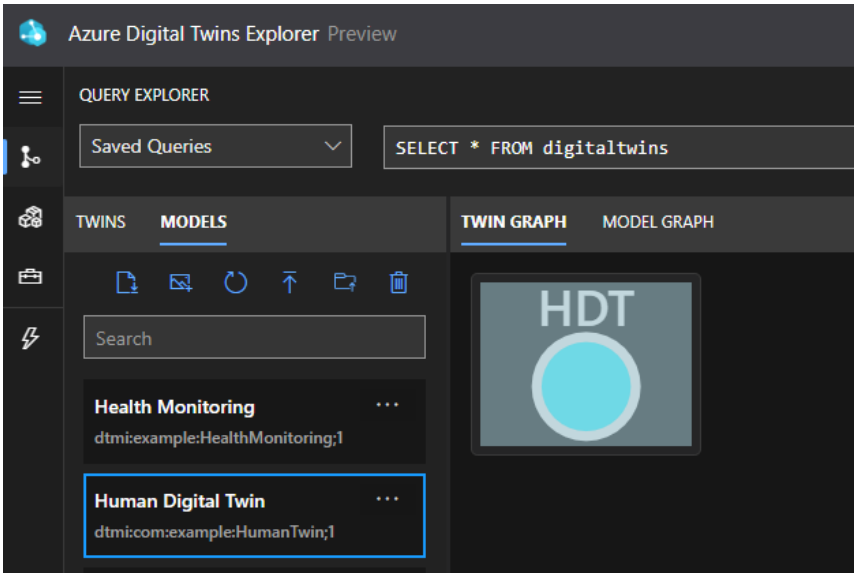

Figure 4.7: HDT of Patient

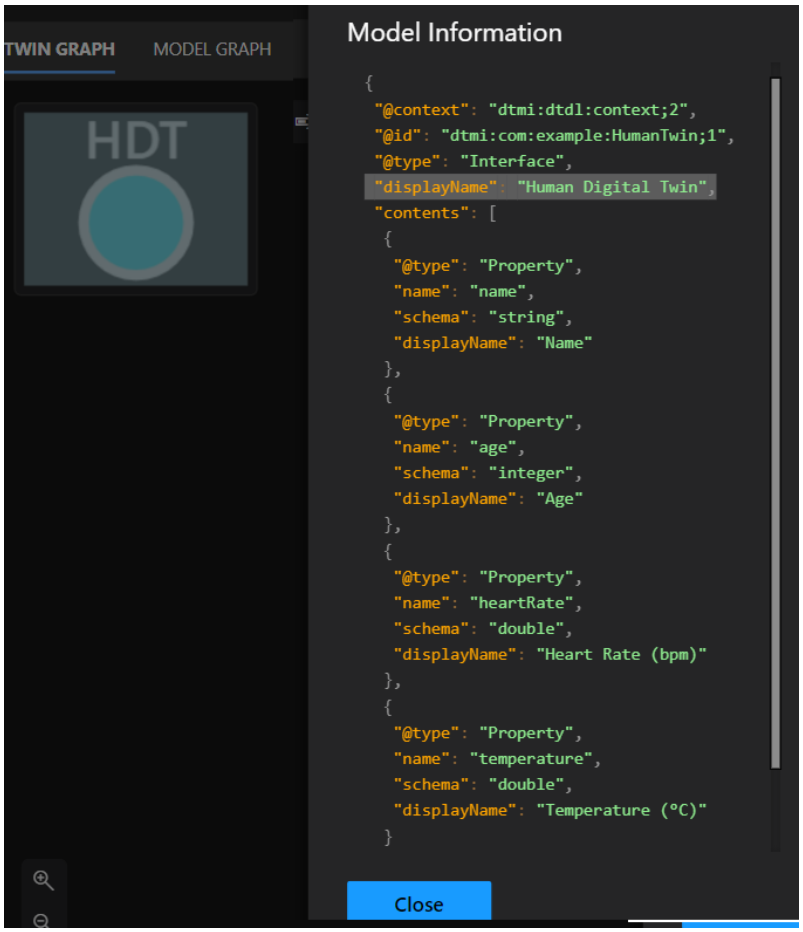

Figure 4.8: HDT Model

Step 4: Create OPC UA console application. Firstly add the Nuget Packages required to build and execute the application mentioned in Figure 4.9.

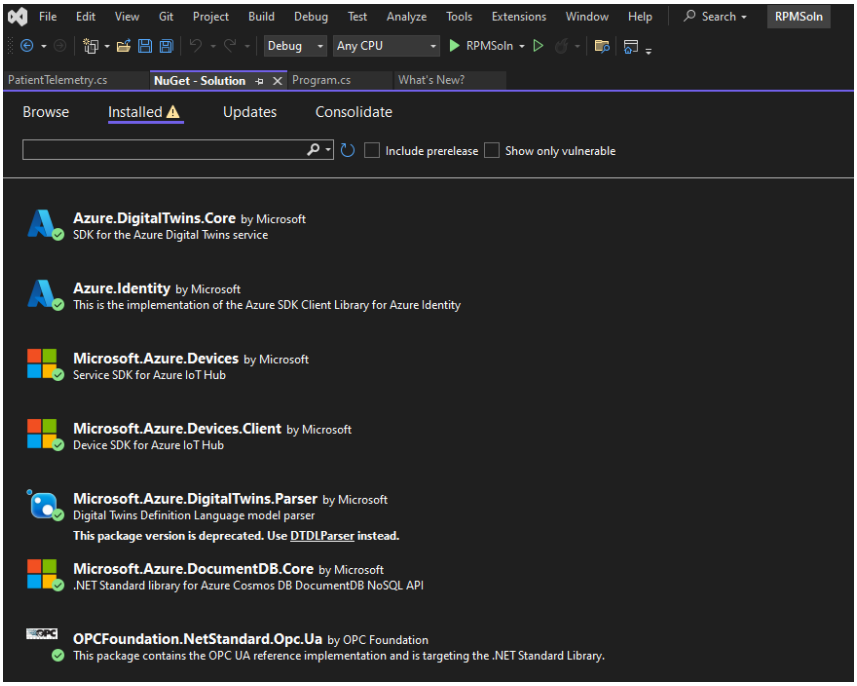

Figure 4.9: Nuget Packages

Step 5: Configure the OPC UA client application to integrate with OPC UA server as coded in Figure 4.10

```
// OPC UA Simulation server endpoint URL
var endpointUrl = "opc.tcp://Windows10:5350/OPCUA/SimulationServer";

// Create a new OPC UA client application configuration
ApplicationConfiguration config = new ApplicationConfiguration()
{
    // Set up application certificate
    ApplicationName = "OPCUA_Simulated_Client",
    ApplicationUri = Utils.Format(@"urn:{0}:OPCUA:Simulated_Client", System.Net.Dns.GetHostName()),
    ApplicationType = ApplicationType.Client,
    SecurityConfiguration = new SecurityConfiguration
    {
        ApplicationCertificate = new CertificateIdentifier(),
        TrustedPeerCertificates = new CertificateTrustList(),
        TrustedIssuerCertificates = new CertificateTrustList(),
        RejectedCertificateStore = new CertificateTrustList(),
        AutoAcceptUntrustedCertificates = true,
    },
    TransportConfigurations = new TransportConfigurationCollection(),
    TransportQuotas = new TransportQuotas { OperationTimeout = 15000 },
    ClientConfiguration = new ClientConfiguration { DefaultSessionTimeout = 60000 },
};

// Create OPC UA application instance
ApplicationInstance application = new ApplicationInstance(config);

var session = await Session.Create(config, new ConfiguredEndpoint(null, new EndpointDescription(endpointUrl)), false, "", 60000, null
```

Figure 4.10: OPC UA To Azure IoT Hub

Step 6: Read the data from the OPC UA Simulation Server through OPC UA client application. The CSharp code snippet for the same is in Figure 4.11.

```
// Retrieve sample patient data from OPC UA Simulation server
string patientName = await ReadPatientData(session, "PatientNameNode");
string name = await ReadPatientData(session, "Name");
int age = int.Parse(await ReadPatientData(session, "Age"));
double temperature = double.Parse(await ReadPatientData(session, "TemperatureNode"));
```

```
4 references
static async Task<string> ReadPatientData(Session session, string nodeId)
{
    // Read patient data from the specified OPC UA node
    ReadValueId nodeToReadValue = new ReadValueId { NodeId = NodeId.Parse(nodeId), AttributeId = Attributes.Value };
    ReadValueIdCollection nodesToRead = new ReadValueIdCollection { nodeToReadValue };
    ReadResponse readResponse = await session.ReadAsync(null, 0, TimestampsToReturn.Neither, nodesToRead,CancellationToken.None);

    // Extract and return the value of the node
    return readResponse.Results[0].ToString();
}
```

Figure 4.11: Reading Data from OPC UA Simulation Server

Step 7: Now, After data is collected from OPC UA server, the pseudonymisation logic is applied to the same. The logic applied to create pseudonyms of the code is shared as shown in Figure 4.12

```
3 references
static string PseudonymiseData(string data)
{
    using (SHA256 sha256Hash = SHA256.Create())
    {
        // Compute hash value of the input data
        byte[] bytes = sha256Hash.ComputeHash(Encoding.UTF8.GetBytes(data));

        // Convert byte array to a string representation of the hexadecimal hash value
        StringBuilder builder = new StringBuilder();
        for (int i = 0; i < bytes.Length; i++)
        {
            builder.Append(bytes[i].ToString("x2"));
        }
        return builder.ToString();
    }
}
```

Figure 4.12: Patient Data Pseudonymization

Step 8: Pseudomnyized data is transmitted to Azure IoT Hub so as to apply the various security policies in the future. Device authentication also takes place at

this stage. The code snippet to integrate with Azure IoT Hub is explained in Figure 4.13

```
var telemetryDataPoint = new
{
    patientName = pseudonymisedName,
    bloodPressure = pseudonymisedBloodPressure,
    age = pseudonymisedAge,
    temperature = pseudonymisedTemperature
};
var messageString = JsonConvert.SerializeObject(telemetryDataPoint);
var message = new Microsoft.Azure.Devices.Client.Message(Encoding.ASCII.GetBytes(messageString));

// Set message properties
message.Properties["messageType"] = "PseudonymisedPatientData";
message.Properties["contentType"] = "application/json";

// Create an instance of the DeviceClient class using the connection string
DeviceClient deviceClient = DeviceClient.CreateFromConnectionString(iotHubConnectionString, Microsoft.Azure.Devices.Client.TransportType.Mqtt);

// Send the message to Azure IoT Hub
await deviceClient.SendEventAsync(message);
Console.WriteLine("Pseudonymised patient data sent to Azure IoT Hub.");
```

Figure 4.13: Pseudonymized Data integration with Azure IoT Hub

Step 9: Create Patient Telemetry Data class. Figure 4.14 contains the code for the class. The Csharp console application is created to subscribe to telemetry messages from the IoT Hub and update the properties of the Human Digital Twin accordingly. The properties of the Human Digital Twin reflect the state of the patient monitoring devices. Telemetry data structure **PatientTelemetry** needs to match the format of the data published by the OPC UA server. This can be achieved by creating Azure Functions, which are also tested.

Step 10: Ingest Data into Human Digital Twin from Azure IoT Hub. The pseudonymized data is ingested into Azure Digital Twin created using DTDL. Figure 4.15 can be referred to understand the code for this functionality.

The data is read from OPC UA to update in the properties of HDT displayed in Figure 4.16 in the final stage.

```
RemotePatientMonitoring.PatientTelemetry
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace RemotePatientMonitoring
{
    1 reference
    public class PatientTelemetry
    {

        0 references
        public double HeartRate { get; set; }
        0 references
        public double BodyTemperature { get; set; }
        1 reference
        public string  PatientName { get; set; } = string.Empty;
        1 reference
        public string BloodPressure { get; set; } = string.Empty;
        1 reference
        public int age { get; set;}
        1 reference
        public double temperature { get; set;}


    }
}
```

Figure 4.14: Telemetry Data

```
1 reference
private static async Task<MessageResponse> OnMessageReceived(Message message, object userContext)
{
    try
    {
        // Parse telemetry data from message
        var telemetryData = JsonConvert.DeserializeObject<PatientTelemetry>(Encoding.UTF8.GetString(message.GetBytes()));

        DigitalTwinsClient adt;

        var cred = new ClientSecretCredential(adtTenantId, adtClientId, adtClientSecret);

        adt = new DigitalTwinsClient(new Uri(adtConnectionString), cred);

        // Update Human Digital Twin properties
        var updateOperations = new JsonPatchDocument();
        if (telemetryData != null)
        {
            updateOperations.AppendReplace("/name", telemetryData.PatientName); // Replace <property-name> with actual property name
            updateOperations.AppendReplace("/age", telemetryData.age);
            updateOperations.AppendReplace("/bloodpressure", telemetryData.BloodPressure);
            updateOperations.AppendReplace("/temperature", telemetryData.temperature);
        }

        await adt.UpdateDigitalTwinAsync(digitalTwinId, updateOperations);

        Console.WriteLine("Telemetry data processed and Human Digital Twin updated successfully.");
    }
    catch (Exception ex)
    {
        Console.WriteLine($"An error occurred while processing telemetry data: {ex.Message}");
    }
```

Figure 4.15: Ingest Data to Azure Digital Twin

Step 11: Send Email notification to Healthcare provider

When the data of the HDT changes and the values are out of the prescribed thresholds, an email notification is sent to the Healthcare Providers who in turn

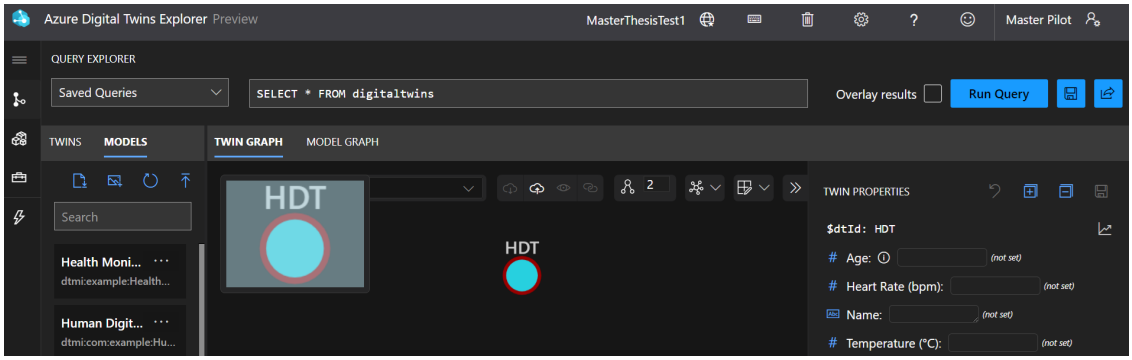

Figure 4.16: Properties of HDT

send notification to nearby caregivers to provide service to the patient.

5 Experimental Evaluation

In the evaluation by Santiago et al., [50], it is observed that OPC UA is capable of handling time-sensitive networks for vital infrastructure and hard communication in real time. Hence, it can be very well considered for real-time patient monitoring. Analysis done by Cavalieri et al.[51] clearly depicts that OPC UA offers a security paradigm with data integrity, encryption, and authentication features. OPC UA is capable of utilizing many transport protocols, including SOAP Web Services over HTTP and UA TCP. Additionally, it supports various encoding standards, including UA Binary and XML/text [51]. These data exchange protocols enable communication that is safe, dependable, and compatible.

5.1 Data Flow

It is critical to understand the dataflow sequence in the Remote Patient Monitoring Model. Figure 5.1 displays the data flow in the proposed SecureHealth RPM system that is compliant and in line with the data flow options mentioned by the NIST publication related to Securing Telehealth Remote Patient Monitoring Ecosystem [2] in Section 4.3.

In the proposed architecture referred to as SecureHealth, the C# console application is created for testing and deployed on localhost IIS. Azure IoT Hub devices and Azure Digital Twin are created on the Azure Web Portal. The Prosys Simulation server is installed on the Windows OS and configured on a Virtual Box instance.

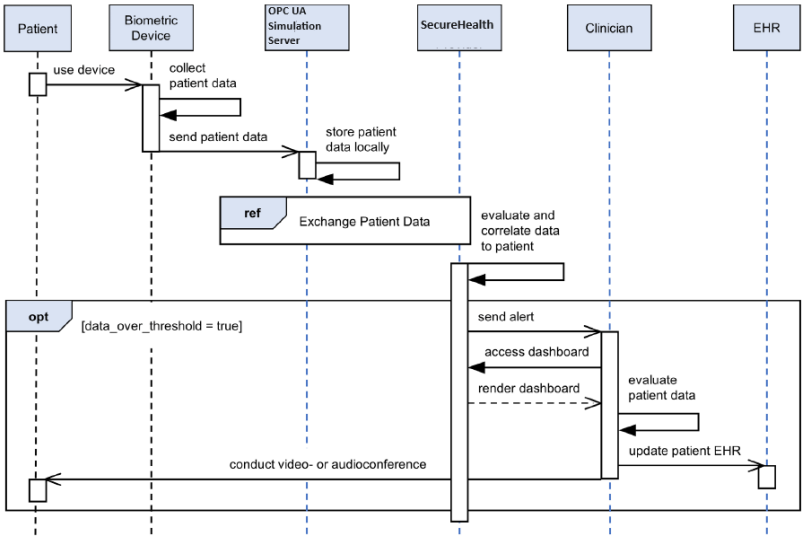

Figure 5.1: Data Flow

5.2 Dataset Description

The collection of the values of sensors from healthcare wearables is a large variety of data. Hence, the process of collecting data from healthcare wearables remote monitoring sensor devices or similar technologies is considered to be out of the scope of this thesis work. The data is collected from the various online medical datasets and is assumed to be acquired correctly. Hence, the scope of this work is to evaluate the cloud-based architecture integrating with OPC UA in the Remote Patient Monitoring (RPM) System.

5.2.1 Dataset I

The first dataset considered for the thesis was downloaded from Kaggle [52]. Ivan et al. [53] considered this dataset for their work to create the synthetic dataset using a Generative Adversarial Network (GAN). The IoMT sensors retrieve the data. For the course of three consecutive months, data is gathered daily. Oxygen, body temperature, heart rate, heart rate master, weight, diastolic and systolic blood

pressure, and many other parameters were included in this data. This data is used in the current thesis work to test the proposed integration on the Cloud. This data was taken as a reference to calculate the MRT(Maximum Response Time) to update the health data of Human Digital Twin.

5.2.2 Dataset II - CVD

The considered dataset is downloaded from Kaggle [54]. This dataset was considered by Chidozie et al. [55] in their research work to improve the prediction and management of cardiovascular disease (CVD), a leading cause of mortality worldwide. This data was collected from MIMIC-III [56] clinical database. Human biophysical parameters form the basis of this dataset under consideration, which are vital markers for tracking and assisting patients with cardiovascular disease (CVD) and enabling both short- and long-term risk assessment. These metrics, which include blood pressure, oxygen saturation, heart rate, and respiration rate, are essential for determining the risk of developing CVD and evaluating general health. The initiative intends to improve early identification, intervention, and management techniques for patients at risk of cardiovascular disease (CVD) by carefully analyzing and interpreting these vital signs. This will help to improve patient outcomes and lower rates of cardiovascular morbidity and death.

5.2.3 Dataset III -Sepsis

This dataset was considered from the work by Shimazui et al. [57]. The data collected for their work consisted of both non-elderly and elderly patients. Patients who are elderly have particular vital signs. The purpose of this study was to determine whether elderly and non-elderly sepsis patients had different relationships between vital signs and death. The patients were divided into two age groups: non-elderly and elderly ($>$75 or =75 or $<$75 years). The body temperature - BT, heart rate,

systolic blood pressure, mean arterial pressure, and respiration rate were the vital signs that the authors examined for correlations with 90-day in-hospital mortality.

5.3 Evaluation Metrics

5.3.1 Calculation of Maximum Response Time (MRT)

In this section, the result of the experimental setup of the proposed architecture is discussed. MRT is referred to here as the time taken to update the values of temperature and heart rate from OPC UA integrated health device data to Human Digital Twin. In SecuerHealth, data from OPC UA integrated healthcare wearable devices is transmitted from Azure IoT Hub to Azure Digital Twin. The goal of testing is to calculate the latency of data transmission. The data taken into consideration is the synthetic data generated based on Dataset I, which is mentioned in section 5.2.1. Using this data, Healthcare Wearable Device Simulation is created in Prosys OPC UA Simulation Server.

This testing is done using two different approaches. First, the OPC UA client application receives data from the OPC UA Simulation Server. A CSharp application was created to receive data from the OPC UA Client and send it to Azure IoT Hub. Then, the data from the Azure IoT Hub device will be updated to the Azure Digital Twin by mapping the device IDs and their properties. The CSharp code setup is done in two systems for testing. The code is tested in the Visual Studio Community version on Windows OS. The next test was done using Visual Studio Code IDE on the Ubuntu OS. The time taken to update through an application on the Azure portal varies from system to system. It should be noted that the first time an application is launched, it takes longer to complete than the second time or more since the first time the application is performed, it needs to create an IIS certificate. In this case, the web application is deployed in the IIS localhost and it

is integrated with the Azure IoT Hub Device connection string and further with the Azure Digital Twin connection string. Another option to test is to create the Azure Function App that can transmit the data from the Azure IoT Hub to Azure Digital Twin.

Second, the health data values of the Human Digital Twin created in Azure Digital Twin are updated in the Azure Digital Twin Explorer. The time taken to update these HDT values is measured in both cases. Table 5.1 shows the data in both cases.

Data Update	**MRT for C# console app**	**MRT for Azure Digital Twin Explorer**
Single Property update	32 ms	3 ms
Multiple Property update	48 ms	5 ms

Table 5.1: MRT for single and multiple data update

The cost evaluation based on MRT for each component can be done as mentioned in the work by Stefan et al. [58]. With the help of Azure Digital Twin, it is possible to build an interactive, real-time representation of all the objects, people, and buildings in actual surroundings.

5.3.2 Statistical Analysis for Privacy-Preserving and Data Security

The proposed system in the thesis is compared to the current Remote Patient Monitoring (RPM) systems. A chi-square test is used to compare the security and privacy policies of the two RPM systems that are being discussed in order to evaluate the security features of existing RPM systems vs. the proposed SecureHealth RPM system. Thus, data privacy and security are crucial elements. Chi-Square test has been previously used in security analysis and anomaly-based detection [59]. Metrics such as data encryption protocols, access controls, audit logging, secure data transfer, and compliance with regulatory standards (e.g., HIPAA) are considered for the

comparison.

5.4 Results and Analysis

In this section, statistical analysis of the two existing RPM systems and the proposed SecureHealth RPM system is executed using the Chi-Square Test. The first work considered is the framework for IoT based Heart rate monitoring [45] and the second framework into consideration is A Real-Time Health Monitoring System for Remote Cardiac Patients Using Smartphone and Wearable Sensors [46].

5.4.1 Comparison of Security Controls

Before the test is performed, the various security controls of all three systems must be compared. Table 5.2 compares the security controls of the systems. Based on the comparison, the proposed architecture appears to have a more comprehensive and robust security approach compared to the IoT-based heart monitoring system and the real-time heart monitoring system using smartphones and wearable sensors. The proposed architecture incorporates advanced security features like data encryption, secure data transfer, access controls, regulatory compliance, and data privacy measures, which are not as prominently featured in the other two systems. The IoT-based heart monitoring system and the real-time heart monitoring system have more basic security controls, such as encryption during data transmission and user authentication for access. However, they lack the depth and breadth of security features present in the proposed architecture, particularly in areas like regulatory compliance, audit logging, and cloud security.

Security Control	**Proposed Architecture (SecureHealth)**	**IoT-Based Heart Monitoring System**	**Real-Time Heart Monitoring System**
Data Encryption	Wearable devices encrypt data before transmission- OPC UA encrypts data using strong algorithms like AES	128-bit encryption applied as a token to the JSON data during transmission	Bluetooth Low Energy (BLE) provides encryption and authentication mechanisms
Secure Data Transfer	Encrypted communication protocols like TLS/SSL used for data transfer- OPC UA uses secure communication profiles	Zigbee protocol used for secure data transmission between devices	Bluetooth Low Energy (BLE) used for secure data transmission between devices
Access Controls	Role-based access controls restrict access to authorized users and applications- Azure Active Directory and RBAC used for access control	Firebase authentication used to verify the device token by generating a custom token with user data	Web interface requires user ID and password for data visibility
Regulatory Compliance	Wearable devices comply with FDA, MDR, IMDRF regulations- Azure cloud services are compliant with HIPAA, FedRAMP, SOC	Not mentioned	Not mentioned
Data Privacy	Sensitive data fields are replaced with pseudonyms (pseudonymization)	Firebase Security Rules	Web interface requires user authentication, suggesting some data privacy measures
Audit Logging	Device usage and data access events are logged for auditing- Azure IoT Hub and Digital Twins provide audit logs	Not mentioned	Not mentioned
Cloud Security	Azure IoT Hub and Digital Twins leverage Azure cloud security features and compliance certifications	Not mentioned	Not mentioned
OPC UA Security	OPC UA provides secure communication profiles, user authentication and authorization	Not mentioned	Not mentioned

Table 5.2: Comparison of Security Contols

5.4.2 Chi-Square Test for Security and Privacy Metrics

A statistical analysis using the Chi-square test can be performed to compare the security and privacy controls of the two existing RPM systems with those of the

SecureHealth RPM system.

The steps for performing this test can be summarized as:

- Formulating hypotheses specific to the security factors being compared.
- Choosing appropriate statistical tests. In the proposed work, the chi-square test is considered.
- Collecting security-related data for both RPM systems.
- Calculating summary statistics and visualizing the data.
- Performing the hypothesis test and interpreting the results to determine if there is a significant difference in security between the two systems.

5.4.3 Chi-Square Test Results

To compare the security and privacy controls of all three RPM systems, the metrics considered are Data Encryption, Access Controls, Secure Data Transfer, Data Privacy, Regulatory Compliance, Cloud Security and Audit Logging.

Step 1: Formulate Hypothesis

- *Null Hypothesis*: There is no significant difference in data privacy and security measures between the existing RPM system and the proposed RPM system.
- *Alternative Hypothesis*: There is a significant difference in data privacy and security measures between the two systems.

Step 2: Prepare Data

Organize the data into a contingency table, also known as a cross-tabulation table or frequency table. The frequency for the Contingency table is calculated based on each security feature provided by the number of Components in the Framework. Data Encryption feature is provided by OPC UA, Pseudonymization, Azure IoT and

Azure DT. Hence, the value of frequency in the contingency table is 4. Similarly, the frequency of other security controls is calculated in the system. Table 5.3 displays the contingency table.

Security Control	Proposed Architecture	IoT-Based Heart Monitoring System	Real-Time Heart Monitoring System	Total
Data Encryption	4	1	1	6
Access Control	4	1	1	6
Secure Data Transfer	4	1	1	6
Data Privacy	4	0	1	5
Regulatory Compliance	4	0	0	4
Cloud Security	4	0	0	4
Audit Logging	4	0	0	4
Total	28	3	4	35

Table 5.3: Contigency Table

Step 3: Calculate expected frequency

Row totals: Sum of frequencies in each row.

Column totals: Sum of frequencies in each column.

Expected value = (Row total × Column total) / Grand total

For example, the expected value for the cell (Data Encryption, Proposed Architecture) is: Expected value = (6 × 28) / 35 = 4.80

Step 4: Calculate the Chi-Square statistic

The chi-square statistic is calculated for each cell using the formula: ^{2} = [(Observed - Expected)^2 / Expected]

Total Chi-Square Value = [(Observed - Expected)^2 / Expected]

In this case, Chi-Square Value = 42

Step 5: Calculate the degree of freedom

Degrees of freedom (df) = (number of rows - 1) × (number of columns - 1) = (7 - 1) × (3 - 1) = 12

Step 6: Determine Critical Value

Security Control	Proposed Architecture	IoT-Based Heart Monitoring System	Real-Time Heart Monitoring System	Total
Data Encryption	4.80	0.51	0.69	6
Access Control	4.80	0.51	0.69	6
Secure Data Transfer	4.80	0.51	0.69	6
Data Privacy	4.00	0.43	0.57	5
Regulatory Compliance	3.20	0.34	0.46	4
Cloud Security	3.20	0.34	0.46	4
Audit Logging	3.20	0.34	0.46	4
Total	28	3	4	35

Table 5.4: Sum Total for Security Metric Data

To determine the critical value for the chi-square test, we need to consider the significance level, usually denoted as alpha and the degrees of freedom (df).

Using a chi-square distribution table, the critical value for df = 12 and = 0.05 is 21.026.

Step 8: Evaluate and Interpret

Hence, the calculated chi-square value (42.00) is greater than the critical value (21.03), leading to the rejection of the null hypothesis. This indicates a significant difference in the frequencies of the security controls among the three systems.

In the same way, we can also perform the Chi-Square test for latency comparison as well. But as the most accurate data about the latency for the existing remote patient monitoring systems were not available, hence that scenario is not considered in the current work.

6 Discussion

Based on the provided list of existing Remote Patient Monitoring (RPM) systems, none of them explicitly mention the use of Azure IoT and OPC UA technologies in combination. However, it's important to note that specific technology implementations may not always be publicly disclosed or readily available in online materials. While the listed RPM systems may not mention Azure IoT and OPC UA explicitly, some RPM solutions may use similar technologies under the hood for device integration, data transmission, and cloud connectivity.

6.1 Previous Research and Approaches

Majumdar et al. [27] emphasized the critical role of wearable sensors in RPM systems, highlighting their ability to provide continuous, non-invasive monitoring of physiological signs. These sensors can measure electro-physiological signals such as ECG, EEG, GSR, and EMG. However, the study points out the need for robust data security measures, particularly when dealing with sensitive health data. Nora et al. [23] discussed the benefits of RPM systems in reducing healthcare costs and improving patient quality of life through continuous monitoring. Yet, the study lacked detailed security implementations, which are crucial for protecting patient data.

Benedict [29] addressed the challenges of data transfer and communication protocols in RPM systems, proposing the integration of the OPC UA standard to resolve

device interoperability issues and secure data communication. Similarly, Miranda et al. [31] presented the OPC UA as a flexible and robust framework for integrating heterogeneous healthcare systems but did not extensively cover scalability and compatibility with existing systems.

Fernandes et al. [30] and Saranya et al. [37] explored the use of IoT frameworks and digital twin technology in healthcare, respectively. However, their work lacked a comprehensive focus on security controls, particularly in the context of data encryption and privacy protection. Okegbile et al. [32] highlighted the potential of Human Digital Twin (HDT) technology in revolutionizing personalized healthcare but identified challenges related to privacy and security concerns, as well as the need for advanced learning techniques.

6.2 Benefits of the Proposed SecureHealth RPM System

Building upon these studies, this thesis proposes a novel architecture for securing patient data and enhancing personalized healthcare in RPM systems by integrating healthcare wearable device data with the OPC UA standard and leveraging Azure IoT Hub and Azure Digital Twin for advanced data analysis and prediction. The proposed SecureHealth RPM system provides a comprehensive solution for remote patient monitoring, addressing the security, privacy, and latency requirements of healthcare providers and patients. By leveraging OPC UA and Azure Digital Twin, the framework offers a scalable and interoperable platform for remote healthcare delivery. Implementing pseudonymization of the patient data also enables a robust security architecture.

Existing systems face challenges like data security, interoperability issues, and latency in remote patient monitoring. OPC UA addresses these challenges by provid-

ing built-in security features such as encryption and authentication, ensuring secure communication between devices and the cloud. Azure IoT complements this with robust identity management and access control mechanisms, enhancing data security. The convergence of OPC UA and Azure IoT bridges the gap between Operational Technology (OT) and Information Technology (IT), enabling real-time monitoring and predictive analytics in remote patient monitoring systems. OPC UA and Azure IoT can help resolve challenges in remote patient monitoring systems by ensuring secure data exchange, real-time analytics, and predictive maintenance capabilities. By leveraging OPC UA-enabled devices feeding data to Azure IoT, industries can implement predictive maintenance strategies, reducing downtime and enhancing operational efficiency. The seamless integration of OPC UA with Azure IoT offers transformative advancements in remote patient monitoring, empowering industries to harness the full potential of IoT data securely and efficiently. Creating Human Digital Twin using Digital Twin Definition Language provides the flexible and scalable feature to create the HDT for n number of patients and n number of data for one or many patients. Additionally, implementing the logic of the pseudonymization technique ensures data security.

The proposed SecureHealth RPM system that implements OPC UA, Azure IoT and Azure Digital Twin can offer several benefits compared to existing RPM systems. They are listed as following in brief:

1. Interoperability and Standardization: Regardless of the manufacturers or communication interfaces of various healthcare equipment, OPC UA offers a common communication protocol for connecting them. This OPC UA interoperability capability guarantees smooth data interchange within the RPM system and makes device integration easier.OPC UA resolves the issue of device interoperability and provides secure communication channels, as discussed by Benedict [29] and Miranda et al. [31].

2. Scalability and Flexibility: Large volumes of patient data may be managed and processed with ease with Azure IoT's scalable and adaptable cloud-based infrastructure. The IoT Hub and database services provided by Azure enable the RPM system to handle an increasing number of patients and devices while preserving excellent performance and dependability.

3. Real-time Data Processing and Analytics: The real-time data processing capabilities of Azure IoT facilitate the analysis of patient data as it is received by the RPM system, hence enabling prompt detection of abnormalities, trends, and key occurrences. This makes proactive healthcare actions possible and enhances patient outcomes through the early detection and resolution of health problems. Azure IoT facilitates real-time device and/or patient condition monitoring. Additionally, it assists in determining the need for maintenance before problems arise and boosts uptime while decreasing unscheduled downtime. With rich visualizations and an all-encompassing view of a patient's health provided by OPC UA and Azure IoT, an RPM system enables doctors to prioritize patients that require intense care while monitoring many patients on a single RPM dashboard. For those with acute or chronic illnesses that pose a significant risk, the prompt and instantaneous transfer of information can be life-saving.

4. Enhanced Security and Compliance: Azure IoT provides robust security features, including end-to-end encryption, identity management, and access control, to protect patient data from unauthorized access and cyber threats. By leveraging Azure's compliance certifications and built-in security controls, RPM system can meet regulatory requirements such as HIPAA and GDPR, ensuring patient privacy and data protection. The security features of OPC UA, such as certificate-based authentication, also provide a secure foundation for trusted healthcare IoT applications. The proposed architecture employs

pseudonymization techniques. Data from wearable devices is encrypted to prevent unauthorized access during transmission. Pseudonymization ensures that personal identifiers are separated from the data, reducing the risk of privacy breaches. This approach builds upon the security measures suggested by Majumdar et al. **a**nd Nora et al. [28].

5. Integration with Healthcare Ecosystem: The RPM system can take advantage of extra features like predictive analytics, telemedicine, and electronic health record (EHR) integration since Azure IoT interfaces easily with other Azure services and outside healthcare apps. By offering a complete healthcare solution, this connection improves the RPM system's entire value proposition.

6. Cost-effectiveness and Time-to-market: Through the use of pre-built IoT services and Azure's pay-as-you-go pricing model, RPM solution can reduce upfront infrastructure expenses and shorten time-to-market. Azure's managed services free up team members to concentrate on creating cutting-edge features and enhancing patient care by lowering the operational burden of managing infrastructure.

7. Comprehensive Digital Representation: Azure Digital Twin offers a thorough digital depiction of patient data and medical equipment. With the help of this depiction, healthcare providers and hospitals may get a comprehensive understanding of the whole RPM ecosystem and track patient health, device performance, and environmental factors in real-time. Azure Digital Twin enables contextual comprehension and connection of diverse data sources by modelling the patient data as digital twins. Individual patient profiles are modelled to construct the "Human Digital Twin" in Azure Digital Twin. This includes digitally recording the vital signs, medical history, treatment plans, and demographics of the patients. Patients' health states can be remotely monitored

by caregivers, who can also keep track of any changes in the patient's condition over time and act quickly if needed. Understanding the connections between ambient variables, device telemetry, and patient health measures can help hospitals and caregivers make better decisions and provide more individualized treatment. RPM systems can use predictive analytics to foresee probable health risks and anticipate device failures by utilizing past data saved in Azure Digital Twin. The primary characteristic of HDT creation is the compatibility and integration of Azure Digital Twin with third-party platforms, industry standards, and other Azure services. A unified and interconnected healthcare environment is ensured by this interoperability, which permits smooth data flow across medical equipment, electronic health record (EHR) systems, telehealth platforms, and RPM apps.

Overall, the SecureHealth RPM system can provide several benefits, including accelerating the implementation of innovative RPM solutions, providing a secure foundation for trusted IoT applications, enabling smart healthcare concepts for predictive healthcare emergencies, and providing a holistic picture of a patient's health with rich visualizations. OPC UA, Azure IoT and Azure DT offer several advantages, including interoperability, scalability, real-time analytics, enhanced security, compliance, integration with the healthcare ecosystem, and cost-effectiveness. These benefits can lead to improved patient outcomes, increased efficiency, and better healthcare delivery compared to existing RPM systems.

6.3 Key Contributions of SecureHealth

The proposed SecureHealth RPM system offers a comprehensive approach to securing patient data and delivering personalized remote patient monitoring. This holistic solution addresses multiple challenges in the field of eHealth and remote

healthcare, representing a significant advancement beyond existing research. The proposed architecture makes several key scientific contributions, as listed in Table 6.1.

Key Contributions	**Explanation**
Integration of Healthcare Devices with OPC UA	OPC UA protocol enables seamless communication and interoperability between diverse healthcare devices, ensuring the efficient collection and transmission of patient data in real-time.
Pseudonymization of Patient Data	We implement robust pseudonymization techniques to anonymize sensitive patient data, protecting patient privacy while facilitating data analysis and transmission to cloud-based platforms.
Utilization of Azure IoT Hub and Azure Digital Twin	SecureHealth RPM system leverages the capabilities of Azure IoT Hub and Azure Digital Twin to store, process, and analyze pseudonymized patient data. This enables real-time monitoring, predictive analytics, and proactive intervention for caregivers and hospitals.
Enhanced Security and Privacy Measures	Data security and privacy are prioritized throughout the SecureHealth RPM system, implementing encryption, access controls, and compliance mechanisms to safeguard patient information and comply with regulatory requirements.
Statistical Analysis Results	Comparison and analysis using the Chi-Square test have provided compelling evidence of the enhanced security offered by the SecureHealth RPM system compared to existing RPM systems.
Addressing Regulatory Compliance	The architecture is designed to comply with stringent data protection regulations, ensuring that patient data is handled lawfully and ethically.
Future-ready Infrastructure	Lays the groundwork for future integration with artificial intelligence and machine learning technologies for more sophisticated data analysis and predictions.

Table 6.1: Key Contributions

The integration of these security and personalization features within the Azure IoT Hub and Azure Digital Twins ecosystem ensures that patient data is protected while enabling the delivery of next-generation, data-driven healthcare solutions that can improve patient outcomes.

6.4 Security Compliance

Azure IoT Hub and Azure Digital Twin are both certified compliant with ISO/IEC 27001, an international standard for information security management systems (ISMS). This certification demonstrates that Azure IoT Hub and Azure Digital Twin follow best practices for managing security risks and protecting information assets. Azure IoT Hub complies with ISOIEC 27018, a code of practice for protecting personally identifiable information (PII) in public cloud services. This certification ensures that Azure IoT Hub adheres to strict privacy controls and safeguards for customer data. Both can be used in HIPAA-compliant healthcare applications and services when configured appropriately. Azure provides a HIPAA Business Associate Agreement (BAA) to customers who require HIPAA (Health Insurance Portability and Accountability Act) compliance for their healthcare solutions. Azure IoT Hub supports GDPR compliance for customers processing the personal data of EU residents.

Data governance and compliance initiatives within a business may also necessitate encryption at rest. Regulations from the government and business world, like FedRAMP, PCI, and HIPAA, specify data security measures and encryption specifications. Some of those standards demand encryption at rest as a necessary precaution. Encryption at rest offers defence-in-depth protection in addition to meeting legal and regulatory standards. A compliant platform for services, apps, and data is offered by Microsoft Azure. In-depth data access control, audits, and physical and facility security are also included.

6.4.1 NIST Compliance

The NIST SPECIAL PUBLICATION 1800-30B [2] focuses on "Securing Telehealth Remote Patient Monitoring Ecosystem." This publication provides a comprehensive guide that demonstrates a standards-based reference design to enhance the security of remote patient monitoring systems in the healthcare sector. It outlines the

approach, architecture, and security characteristics necessary to safeguard patient data and ensure system integrity in telehealth environments. Overall, NIST SP 1800-30B provides detailed implementation guidance for securing RPM systems. It includes recommendations for securing medical devices, implementing network security controls, encrypting data, and implementing access controls. In the proposed architecture, secure communication channels are established between IoT devices, OPC UA servers, and healthcare systems to prevent data breaches and unauthorized access. Hence, it is in line with the secure communication requirements outlined in NIST SP 1800-30B.

6.4.2 Security Controls and NIST Mapping

NIST SP 1800-30B [2] provides a holistic framework for addressing security challenges in RPM systems. By aligning with these guidelines, the proposed architecture ensures that all critical aspects of security are considered, from asset management to incident response. Aligning with this approach helps in prioritizing security measures based on the specific risks associated with remote patient monitoring, ensuring efficient use of resources. By following these guidelines, the architecture incorporates best practices for securing RPM systems, benefiting from the collective expertise of NIST and industry professionals. With a focus on data security and privacy, aligning with NIST SP 1800-30B ensures robust protection of sensitive patient data throughout its lifecycle in the RPM system. The guidelines provide a framework for ongoing risk assessment, helping to identify and address new security challenges as they emerge.

Based on the NIST SP 1800-30B guidelines and the proposed architecture for securing patient data in remote patient monitoring (RPM), Table 6.2 provides an analysis of how the architecture aligns with these guidelines:

NIST-SP 1800-30B Component	**SecureHealth RPM System Alignment**
Identify	The architecture includes an inventory of healthcare wearable devices and data flows, aligning with the asset management aspect of the Identify function.
Protect	The use of OPC UA for secure data transmission aligns with the data security guidelines. Pseudonymization of patient data before cloud transfer addresses the information protection requirements. Azure IoT Hub's security features align with access control recommendations.
Detect	- Continuous monitoring of data flows in Azure IoT Hub aligns with the anomalies and events detection guidelines. Azure Digital Twin analytics can be used for continuous security monitoring as recommended.
Respond	The architecture should include an incident response plan for data breaches and procedures for handling de-pseudonymization requests, as per the response planning guidelines.
Recover	Backup and restore procedures for Azure services, along with data recovery plans for OPC UA systems, align with the recovery planning recommendations.

Table 6.2: NIST SP 1800-30B Mapping

6.5 Challenges and Limitations

Although the proposed architecture incorporates state-of-the-art encryption techniques and strict data pseudonymization protocols, the inherent risks associated with cloud-based services cannot be entirely eliminated.

For the proposed SecureHealth RPM system, experimental setup is a bit complicated process to integrate health data from OPC UA Simulation server with Azure cloud components due to the need to create the OPC UA client application and Azure Functions for data transmission. Proper care needs to be taken for health data and HDT mapping for monitoring. Any error in the parameter mapping will cause the incorrect display of the HDT data and result in incorrect prediction and analysis. Although cloud technology may simplify the operation of the healthcare sector, some medical experts or staff members may require a significant amount of time to grasp the operations of its numerous resources. This can result in the overuse of cloud resources and inaccurate analysis of patient records [60]. A few of

the limitations of the Cloud-based solution are displayed in Figure 6.1

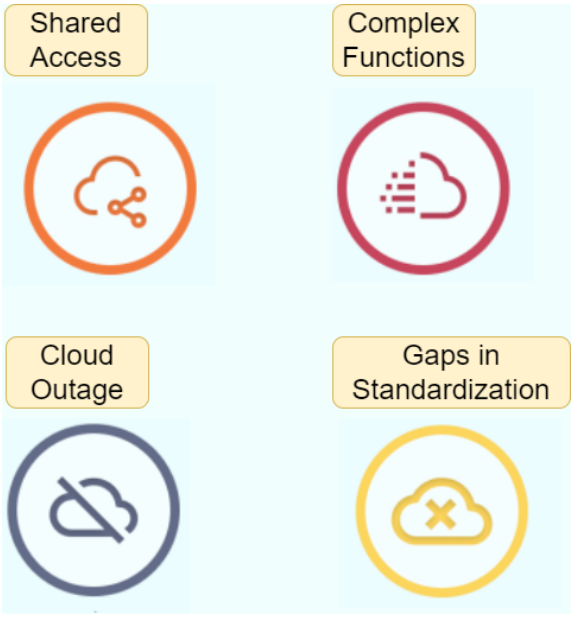

Figure 6.1: Limitations of Cloud-based solutions

The suggested architecture incorporates several layers of security, such as encryption, pseudonymization, and cloud-based services. To guarantee that all security measures work as intended, these layers must be monitored continuously, updated on a regular basis, and workers trained. This complexity can lead to vulnerabilities in security if not managed appropriately, as underlined by the requirement for "ongoing training and awareness programs to mitigate security risks" [61].

When using cloud-based RPM to transport data stored in the cloud, it is possible to break local regulations. The dynamic nature of cloud computing makes it extremely difficult to predict which precise server or storage device will be used, exacerbating the transborder data flow issue. These transborder data flow limits are a special case that we will address later [62].

Implementing OPC UA can be challenging, particularly for smaller healthcare companies with minimal IT resources. Numerous healthcare institutions depend on legacy hardware and software that might not be OPC UA compatible. Integrating OPC UA into these systems can be complex and costly [63].

One of the most difficult aspects of the HDT is that, while some factors may be tracked to identify specific risks, other human features, such as thoughts, reactions, and behavior, can be somewhat unpredictable because humans are more complicated than manufacturing processes [64]. HDT technology is still maturing to provide the prediction analysis for all human features including infections.

Past research has shown that even in the most secure environments, data breaches remain a constant concern. Because of this, cybersecurity is a dynamic field that requires constant attention to detail and adaptation.

Table 6.3 lists the various limitations of the proposed SecureHealth RPM and possible mitigations.

Limitation/Challenge	**Mitigation Strategy**
Cybersecurity Threats	Implement multi-layered security measures. Continuous monitoring and threat intelligence. Employee cybersecurity training programs.
Data Handling Errors	Staff training on data protection. Implement access controls and data loss prevention tools. Use of automated data handling processes where possible.
Integration with Legacy Systems	Gradual system upgrades and modernization. Regular security patches for legacy systems. Implement additional security layers for legacy systems.
Interoperability Challenges	Adherence to Healthcare Data Standards. Collaboration with device manufacturers for compatibility. Regular testing of interoperability and data exchange.
Insider Threats	Implement the principle of least privilege. Regular access audits and monitoring. Employee background checks Data loss prevention (DLP) tools.

Table 6.3: Limitations and Mitigations

It is usually challenging and resource-intensive to integrate modern technologies with legacy systems, necessitating large investments in training and upgrades. There are still a number of healthcare wearables with proprietary data formats and communication interfaces, even though OPC UA provides a standardized communication

protocol. This variability may make it more difficult for the suggested architecture to integrate and share data seamlessly. Human error is more likely in high-pressure settings and complex healthcare procedures when things go wrong, such as misplacing gadgets that hold private data or transmitting data to the incorrect person.

Adoption of modern cloud services and comprehensive security measures, while required, can result in higher operational costs. One of the most common challenges in healthcare is juggling budgetary limits with the requirement for safe, high-quality healthcare monitoring. Reliability and quality of data are critical components of remote patient monitoring systems. Errors or faults in sensors can have a major effect on clinical results.

Delivery of healthcare services may be hampered by cloud outages or disruptions if the architecture depends entirely on a single cloud platform. Therefore, in order to guarantee service continuation even in the event of an outage, it is crucial to build cloud-based healthcare systems with redundancy and failover capabilities.

7 Future Work

Promising avenues for further research to enhance RPM capabilities were noted in the thesis. There is a lot of promise in combining enhanced Human Digital Twin functions, OPC UA, Azure cloud frameworks, edge computing, and federated learning. These developments can meet changing healthcare needs while ensuring data security and further personalizing healthcare. Future study is suggested to include integration with Azure AI and ML for Federated Learning deployment. Healthcare providers can provide individualized, privacy-preserving, and data-driven care that enhances patient outcomes while adhering to legal requirements and standards for data security and privacy by combining federated learning with digital twin technology and remote patient monitoring using the OPC UA standard. Federated learning aggregates model updates from individual patient devices or edge servers to enable ongoing model enhancement and modification. Over time, the prediction models can adjust to changing patient situations, treatment responses, and advancements in healthcare knowledge thanks to this iterative learning process. Federated learning and Digital Twin technology assist healthcare providers in adhering to regulatory requirements like HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) while guaranteeing patient data privacy and security by decentralizing data processing and storage.

7.1 Integration of Artificial Intelligence (AI)

The potential to improve the functionality of remote patient monitoring systems through the integration of artificial intelligence (AI) is promising. The enormous volumes of data gathered from patient monitoring devices can be used by healthcare providers to get important insights by utilizing AI techniques like machine learning and predictive analytics. Improved patient outcomes and increased operational efficiency can result from using this information to facilitate more proactive and individualized healthcare actions.

7.1.1 Anomaly Detection and Alerting

Algorithms for anomaly detection driven by artificial intelligence (AI) can continuously scan patient data streams for odd trends or departures from standard health metrics. Automated warnings that trigger fast action and intervention can be delivered to caregivers and healthcare practitioners when anomalies are identified. Proactive monitoring can help avoid medical emergencies and lower readmission rates to hospitals.

7.1.2 Predictive Analytics for Early Intervention

Predictive analytics for early intervention is one possible use of AI in remote patient monitoring. Artificial intelligence systems are able to recognize patterns and trends that may point to possible health problems or decline by examining past patient data. Proactive alerts and recommendations can then be sent to caregivers and medical experts, enabling them to intervene early and avoid negative outcomes.

7.1.3 Multi-modal Data Fusion and Anomaly Detection

Examine AI models that can combine data from several sources, such as wearable sensors (smartwatches, activity trackers), electronic health records (EHR) data, and real-time data from medical equipment (via OPC UA). AI may be able to identify intricate anomalous patterns by reviewing this rich tapestry of data, which may be overlooked when looking at individual data streams.

7.1.4 Regulatory Compliance

The FDA's guidelines governing the use of AI in healthcare, the GDPR, HIPAA, and other regulatory standards will all be taken into account when developing future RPM systems. Throughout the data lifetime, this entails maintaining data security, privacy, openness, and responsibility.

7.2 Piloting with Differential Privacy

Differential privacy provides a formal privacy guarantee by introducing randomness (noise) into the data or the results of queries on the data. This ensures that the presence or absence of any single individual's data in the dataset does not significantly affect the output, thereby protecting individual privacy. It would be good practice to introduce differential privacy mechanisms when performing data analysis or generating outputs from pseudonymized data. This ensures that even if an adversary has some auxiliary information, they cannot confidently infer sensitive information about any individual in the dataset.

7.3 Integration of Federated Learning

Federated learning, in conjunction with AI, has great potential to advance remote patient monitoring systems. Federated learning eliminates the need to centralize sensitive patient data by enabling collaborative model training across dispersed data sources, including medical facilities and patient devices. By using the combined knowledge of several datasets, our method protects data security and privacy while building more reliable and broadly applicable AI models.

7.3.1 Collaborative Model Training

By enabling the sharing of model updates amongst participating entities while maintaining local storage and encryption of their source data, federated learning promotes collaborative model training. Federated learning can help healthcare organizations cooperatively train AI models using data from various patient populations in the context of remote patient monitoring. This will improve model accuracy and generalization across various demographics and medical conditions.

7.3.2 Privacy-Preserving Data Sharing

One of the key advantages of federated learning is its privacy-preserving nature, which ensures that sensitive patient data remains protected throughout the model training process. By aggregating model updates instead of raw data, federated learning minimizes the risk of data breaches and unauthorized access. This approach fosters trust among healthcare stakeholders and encourages greater collaboration in research and innovation.

7.3.3 Customized Model Personalization

Federated learning enables customized model personalization for individual patients based on their unique health profiles and treatment preferences. By leveraging locally collected data from patient devices, AI models can adapt and tailor their predictions and recommendations to better align with patient-specific needs and preferences. This personalized approach enhances the effectiveness and relevance of remote patient monitoring interventions.

Advanced AI models that can handle complicated medical data, such as time series, imaging, and genomics data, will be necessary for future RPM systems. To guarantee robustness and generalizability, these models must be trained on a variety of datasets. This will be taken into consideration for future design and analysis of the SecureHealth model.

It is expected that remote monitoring will become an increasingly important component of healthcare. The use of RPM in addressing both acute and chronic diseases will increase as care continues to shift out of hospitals and into more home and community-based settings. The potential effects of these new technologies on patient safety and healthcare operations need to be further investigated. Opportunities exist to comprehend how RPM might affect preserving patient safety, averting unfavourable outcomes, and enhancing patient satisfaction. Finding the patients and clinical scenarios most at risk of receiving unsafe telehealth care, as well as identifying and promoting best practices to guarantee equitable access to safe telehealth, are some recommendations made to better understand the effects of RPM on patient safety. Other recommendations include measuring patient safety outcomes systematically and reporting safety incidents more frequently.

8 Conclusion

The proposed framework for Next-Generation Patient Care harnesses Human Digital Twin technology to deliver personalized healthcare in remote patient monitoring (RPM). This thesis has explored critical research questions surrounding the integration of Human Digital Twin (HDT) technology and secure communication protocols within remote patient monitoring (RPM) systems. The findings provide valuable insights into the effective transmission of sensitive health data, the advantages of HDT in healthcare, and the overall performance of the proposed security architecture. By including advanced security measures and harnessing cutting-edge technologies, this framework has proved its ability to improve the landscape of remote healthcare monitoring through thorough design, analysis, and testing. This framework makes an important scientific addition to the field of eHealth and remote healthcare by addressing the changing needs and challenges of remote patient monitoring and personalized healthcare.

In the proposed thesis, OPC UA was chosen as the best communication protocol due to its strong security features, which included encryption, authentication, and authorization. Other protocols were investigated, including LoRa, Zigbee, MQTT, BLE, and Wi-Fi, but OPC UA stood out due to its complete approach to data security and compatibility. The use of 128-bit data encryption, pseudonymization for data privacy, and token-based authentication guarantees that patient data is safely transported between healthcare wearables, medical devices, and the Human Digital

Twin. These safeguards prevent unauthorized access, data breaches, and maintain data integrity during the transmission process. The investigation concludes that the OPC Unified Architecture (OPC UA) protocol is ideal for safeguarding data transmission in RPM systems. OPC UA provides a strong architecture for secure communication, including authentication, encryption, and data integrity. These protocols successfully reduce the risks associated with data breaches and illegal access, which are crucial for patient confidentiality and security.

OPC UA, with its built-in security characteristics, can be used to establish secure communication channels between medical equipment and cloud services. OPC UA reduces the danger of cyberattacks by introducing secure authentication procedures and encryption protocols that allow only authorized devices to connect with the cloud. Complex data formats can also be handled by OPC UA, which facilitates the smooth integration of different medical equipment and improves interoperability while upholding strict security protocols. By utilizing these OPC UA capabilities, it assures that communication between medical devices and the cloud is secure, dependable, and in accordance with industry standards.

The incorporation of Human Digital Twin technology in healthcare has several benefits, such as tailored monitoring, predictive analytics, and improved decision-making capabilities. By developing a virtual representation of patients, healthcare providers can continuously watch health measurements and anticipate potential health issues before they occur. This proactive strategy not only improves patient outcomes, but it also maximizes resource use in healthcare systems. Furthermore, HDT enables individualized treatment regimens based on individual patient data, resulting in more effective treatments and higher patient satisfaction. By eliminating the need for recurrent hospital visits and facilitating prompt medical actions, HDT enables ongoing remote monitoring of the health situations of patients. HDT in RPM lowers healthcare expenditures by reducing hospitalizations and optimizing

resource usage.

The integration of Azure Digital Twin Explorer within the proposed architecture significantly enhances the capabilities of monitoring, analytics, prediction, and decision-making. Azure Digital Twin Explorer functions as a dynamic interface, offering a comprehensive platform for visualizing and interacting with Human Digital Twin. Through this interface, real-time patient data monitoring becomes extremely effective, allowing for timely interventions and ongoing care. The visual depiction of patient data in the form of digital twins allows for a better understanding of patient conditions and helps to discover trends and anomalies. Azure Digital Twin offers the detection of potential health issues before they occur by evaluating patterns in heart rate and temperature data. Such predictive analytics can proactively notify medical personnel, improving patient care. Azure Digital Twin Explorer aids decision-making with advanced modeling that replicates many situations and their effects. These models can help healthcare providers make informed judgments about treatment plans and actions, resulting in more individualized and accurate care for each patient. Azure Digital Twin Explorer plays a crucial role in improving the overall effectiveness of remote patient monitoring systems because of its ability to provide real-time monitoring, sophisticated analytics, and predictive modeling.

The suggested security architecture significantly improves security effectiveness when compared to existing RPM systems. The design successfully protects sensitive patient data against unwanted access and breaches by implementing pseudonymization. The Chi-Square test used in this study shows that the suggested design considerably improves the security aspects of RPM systems by addressing weaknesses reported in existing techniques. Furthermore, the architecture's connection with known cybersecurity standards, such as NIST recommendations, ensures a thorough approach to risk management and regulatory compliance. The architecture offers scalable deployment, allowing for an increasing number of devices and data

volume without sacrificing performance. The system provides consistent and reliable data transfer, which is critical for accurate real-time monitoring and analysis.

Future work will concentrate on improving the privacy and security of the proposed architecture by including sophisticated techniques like federated learning and differential privacy. Federated learning will enable decentralized data analysis, keeping sensitive data on local devices while benefiting from global insights. Differential privacy will provide an additional layer of data protection by adding noise into the data, making it impossible to identify individual patients while retaining the data's utility for analysis and prediction. Future work aims to further enhance its capabilities through the integration of advanced AI and machine learning, expansion of wearable device compatibility, and optimization for large-scale deployments. By continuously improving data privacy and security measures, refining the user experience, and ensuring regulatory compliance, the framework is well-positioned to meet the evolving needs of the healthcare industry.

Overall, the proposed architecture offers a huge step forward in safe and personalized healthcare, utilizing cutting-edge technologies to improve patient outcomes and strengthen data security in remote patient monitoring systems. This study emphasizes the necessity of secure communication protocols and the Human Digital Twin in revolutionizing remote patient monitoring. By tackling fundamental security concerns in healthcare, the suggested architecture improves data privacy while simultaneously paving the path for more tailored and effective patient care in the digital health landscape. By addressing current challenges and anticipating future needs, it lays a solid foundation for the next generation of patient care, ultimately improving the health and well-being of patients worldwide.

References

[1] R. Pekmezaris, I. Mitzner, K. R. Pecinka, C. N. Nouryan, M. L. Lesser, M. Siegel, J. W. Swiderski, G. Moise, R. Younker, and K. Smolich, "The impact of remote patient monitoring (telehealth) upon medicare beneficiaries with heart failure", *Telemedicine and e-Health*, vol. 18, no. 2, pp. 101–108, 2012, PMID: 22283360. DOI: 10.1089/tmj.2011.0095.

[2] NCCOE, *Nist special publication 1800-30b, securing telehealth remote patient monitoring ecosystem*, https://www.nccoe.nist.gov/sites/default/files/legacy-files/rpm-nist-sp1800-30-2nd-draft.pdf, [Accessed 25-03-2024], 2022.

[3] S. Y. Tan, J. Sumner, Y. Wang, and A. Wenjun Yip, *A systematic review of the impacts of remote patient monitoring (RPM) interventions on safety, adherence, quality-of-life and cost-related outcomes - npj Digital Medicine — doi.org*, https://doi.org/10.1038/s41746-024-01182-w, [Accessed 24-07-2024].

[4] S. Razdan and S. Sharma, "Internet of medical things (iomt): Overview, emerging technologies, and case studies", *IETE Technical Review*, vol. 39, no. 4, pp. 775–788, 2022. DOI: 10.1080/02564602.2021.1927863.

[5] *Nccoe.nist.gov*, https://www.nccoe.nist.gov/sites/default/files/legacy-files/hit-th-project-description-final.pdf, [Accessed 30-03-2024].

[6] S. Zulj, G. Seketa, D. Dzaja, F. Sklebar, S. Drobnjak, L. Celic, and R. Magjarevic, "Supporting diabetic patients with a remote patient monitoring systems", in *VII Latin American Congress on Biomedical Engineering CLAIB 2016, Bucaramanga, Santander, Colombia, October 26th-28th, 2016*, Springer, 2017, pp. 577–580.

[7] Z. Yang, Q. Zhou, L. Lei, K. Zheng, and W. Xiang, "An iot-cloud based wearable ecg monitoring system for smart healthcare", *Journal of medical systems*, vol. 40, pp. 1–11, 2016.

[8] B. Daly, T. S. Lauria, J. C. Holland, J. Garcia, J. Majeed, C. B. Walters, M. Zablocki, K. Chow, O. Strachna, C. E. Giles, *et al.*, "Oncology patients' perspectives on remote patient monitoring for covid-19", *JCO Oncology Practice*, vol. 17, no. 9, e1278–e1285, 2021.

[9] U. Nations, *World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100 | United Nations — un.org*, `https://www.un.org/en/desa/world-population-projected-reach-98-billion-2050-and-112-billion-2100`, [Accessed 23-04-2024].

[10] Y. Liu, L. Zhang, Y. Yang, L. Zhou, L. Ren, F. Wang, R. Liu, Z. Pang, and M. J. Deen, "A novel cloud-based framework for the elderly healthcare services using digital twin", *IEEE access*, vol. 7, pp. 49 088–49 101, 2019.

[11] *Psychotherapy centre's database hacked, patient info held ransom — yle.fi*, `https://yle.fi/a/3-11605460`, [Accessed 24-07-2024].

[12] *As Hackers Take Down Newfoundland's Health Care System, Silence Descends (Published 2021) — nytimes.com*, `https://www.nytimes.com/2021/11/12/world/canada/newfoundland-cyberattack.html`, [Accessed 24-07-2024].

[13] H. W. Jessie Yeung, *Australia sanctions Russian national accused of hacking in Medibank data leak | CNN Business — edition.cnn.com*, `https://edition.`

cnn.com/2024/01/23/tech/medibank-attack-australia-sanction-revil-intl-hnk/index.html, [Accessed 24-07-2024].

[14] *HCA Healthcare Reports Data Security Incident — investor.hcahealthcare.com*, https://investor.hcahealthcare.com/news/news-details/2023/HCA-Healthcare-Reports-Data-Security-Incident/default.aspx, [Accessed 24-07-2024].

[15] R. van Kessel, M. Haig, and E. Mossialos, "Strengthening cybersecurity for patient data protection in europe", *Journal Of Medical Internet Research*, vol. 25, e48824, Aug. 2023, ISSN: 1438-8871.

[16] M. Shafto, M. Conroy, R. Doyle, E. Glaessgen, C. Kemp, J. LeMoigne, and L. Wang, "Draft modeling, simulation, information technology & processing roadmap", *Technology area*, vol. 11, pp. 1–32, 2010.

[17] B. Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart, and A. Calomino, "Materials, structures, mechanical systems, and manufacturing roadmap", *NASA TA*, pp. 12–2, 2012.

[18] Y. Zheng, S. Yang, and H. Cheng, "An application framework of digital twin and its case study", *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 1141–1153, 2019.

[19] B. R. Barricelli, E. Casiraghi, and D. Fogli, "A survey on digital twin: Definitions, characteristics, applications, and design implications", *IEEE access*, vol. 7, pp. 167 653–167 671, 2019.

[20] E. Katsoulakis, Q. Wang, H. Wu, L. Shahriyari, R. Fletcher, J. Liu, L. Achenie, H. Liu, P. Jackson, Y. Xiao, *et al.*, "Digital twins for health: A scoping review", *NPJ Digital Medicine*, vol. 7, no. 1, p. 77, 2024.

[21] A. Vallée, "Digital twin for healthcare systems", *Frontiers in Digital Health*, vol. 5, p. 1 253 050, 2023.

[22] B. R. Barricelli, E. Casiraghi, J. Gliozzo, A. Petrini, and S. Valtolina, "Human digital twin for fitness management", *IEEE Access*, vol. 8, pp. 26 637–26 664, 2020.

[23] W. Mahnke, S.-H. Leitner, and M. Damm, *OPC unified architecture*. Springer Science & Business Media, 2009.

[24] K. Wallis, M. Merzinger, C. Reich, and C. Schindelhauer, "A security model based authorization concept for opc unified architecture", in *Proceedings of the 10th International Conference on Advances in Information Technology*, Bangkok, Thailand, 2018, pp. 1–8.

[25] C. Newton-Smith, *Reimagining healthcare with Azure IoT | Microsoft Azure Blog — azure.microsoft.com*, `https://azure.microsoft.com/en-us/blog/reimagining-healthcare-with-azure-iot/`, [Accessed 23-04-2024].

[26] *IoT in Healthcare Solutions | Microsoft Azure azure.microsoft.com*, `https://azure.microsoft.com/en-us/solutions/healthcare-iot`, [Accessed 23-04-2024].

[27] S. Majumder, T. Mondal, and M. J. Deen, "Wearable sensors for remote health monitoring", *Sensors*, vol. 17, no. 1, p. 130, 2017.

[28] N. El-Rashidy, S. El-Sappagh, S. R. Islam, H. M. El-Bakry, and S. Abdelrazek, "Mobile health in remote patient monitoring for chronic diseases: Principles, trends, and challenges", *Diagnostics*, vol. 11, no. 4, p. 607, 2021.

[29] S. Benedict, "IoT Enabled Remote Monitoring Techniques for Healthcare Applications-An Overview", *Informatica*, vol. 46, no. 2, 2022.

[30] C. O. Fernandes and C. J. P. De Lucena, "A software framework for remote patient monitoring by using multi-agent systems support", *JMIR medical informatics*, vol. 5, no. 1, e6693, 2017.

[31] J. Miranda, J. Cabral, S. Banerjee, D. Grossmann, C. F. Pedersen, and S. R. Wagner, "Analysis of opc unified architecture for healthcare applications", in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE, Limassol, Cyprus, 2017, pp. 1–4.

[32] S. D. Okegbile, J. Cai, C. Yi, and D. Niyato, "Human digital twin for personalized healthcare: Vision, architecture and future directions", *IEEE network*, 2022.

[33] G. A. Vargas, "Personalized healthcare: How to improve outcomes by increasing benefit and decreasing risk through the use of biomarkers", *Biomarkers in Medicine*, vol. 3, no. 6, pp. 701–709, 2009. DOI: 10.2217/bmm.09.74.

[34] L. P. Malasinghe, N. Ramzan, and K. Dahal, "Remote patient monitoring: A comprehensive study", *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 57–76, 2019.

[35] K. Boikanyo, A. M. Zungeru, B. Sigweni, A. Yahya, and C. Lebekwe, "Remote patient monitoring systems: Applications, architecture, and challenges", *Scientific African*, vol. 20, e01638, 2023, ISSN: 2468-2276. DOI: https://doi.org/10.1016/j.sciaf.2023.e01638.

[36] S. Greene, H. Thapliyal, and D. Carpenter, "Iot-based fall detection for smart home environments", in *2016 IEEE international symposium on nanoelectronic and information systems (iNIS)*, IEEE, Gwalior, India, 2016, pp. 23–28.

[37] S. Saranya, N. Kanimozhi, and C. Santhosh, "Digital twins in e-health: Adoption of technology and challenges in the management of clinical systems", *Digital Twin Technologies for Healthcare 4.0*, vol. 46, p. 53, 2023.

[38] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology", in *2006 international conference of the*

IEEE engineering in medicine and biology society, IEEE, New York, NY, USA, 2006, pp. 5453–5458.

[39] U. Hariharan, K. Rajkumar, T. Akilan, and J. Jeyavel, "Smart wearable devices for remote patient monitoring in healthcare 4.0", *Internet of Medical Things: Remote Healthcare Systems and Applications*, pp. 117–135, 2021.

[40] *New Wearable Communication System Offers Potential to Reduce Digital Health Divide — news.engineering.arizona.edu*, https://news.engineering.arizona.edu/news/new-wearable-communication-system-offers-potential-reduce-digital-health-divide, [Accessed 11-04-2024].

[41] *What is OPC UA- Quick Guide & FAQ — page.advantech.com*, https://page.advantech.com/en/global/industrial-automation/industrial-io/opc-ua, [Accessed 30-03-2024].

[42] *Art. 4 GDPR – Definitions - General Data Protection Regulation (GDPR) — gdpr-info.eu*, https://gdpr-info.eu/art-4-gdpr/, [Accessed 18-07-2024].

[43] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "Pax: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system", *International Journal of Environmental Research and Public Health*, vol. 16, no. 9, p. 1490, 2019.

[44] msmbaldwin, *Azure Data Encryption-at-Rest - Azure Security learn.microsoft.com*, https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest, [Accessed 23-04-2024].

[45] M. Umer, T. Aljrees, H. Karamti, A. Ishaq, S. Alsubai, M. Omar, A. K. Bashir, and I. Ashraf, *Heart failure patients monitoring using IoT-based remote monitoring system - Scientific Reports — nature.com*, https://www.nature.com/articles/s41598-023-46322-6, [Accessed 15-07-2024].

[46] P. Kakria, N. Tripathi, and P. Kitipawong, "A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors", *International Journal of Telemedicine and Applications*, vol. 2015, pp. 1–11, Dec. 2015. DOI: 10.1155/2015/373474.

[47] *OPC UA - The Security Solution for the Internet of Things; OPC Connect, opcconnect.opcfoundation.org*, https://opcconnect.opcfoundation.org/2018/04/opc-ua-the-security-solution-for-the-internet-of-things/, [Accessed 15-07-2024].

[48] Dominicbetts, *Connect industrial assets using Azure IoT OPC UA Broker - Azure IoT Operations Preview — learn.microsoft.com*, https://learn.microsoft.com/en-us/azure/iot-operations/manage-devices-assets/overview-opcua-broker, [Accessed 15-07-2024].

[49] Baanders, *DTDL models - Azure Digital Twins - learn.microsoft.com*, https://learn.microsoft.com/en-us/azure/digital-twins/concepts-models, [Accessed 23-04-2024].

[50] S. Gil, G. D. Zapata-Madrigal, R. García-Sierra, and L. A. Cruz Salazar, *Converging IoT protocols for the data integration of automation systems in the electrical industry - Journal of Electrical Systems and Information Technology — jesit.springeropen.com*, https://jesit.springeropen.com/articles/10.1186/s43067-022-00043-4, [Accessed 30-03-2024].

[51] S. Cavalieri and F. Chiacchio, "Analysis of opc ua performances", *Computer Standards & Interfaces*, vol. 36, no. 1, pp. 165–177, 2013.

[52] *BPCO dataset based GANs for IoMT — kaggle.com*, https://www.kaggle.com/datasets/cnrieiit/bpco-dataset-based-gans-for-iomt?resource=download, [Accessed 09-04-2024].

[53] I. Vaccari, V. Orani, A. Paglialonga, E. Cambiaso, and M. Mongelli, "A generative adversarial network (gan) technique for internet of medical things data", *Sensors*, vol. 21, no. 11, p. 3726, 2021.

[54] $CVD_Vital_Signs - kaggle.com$, https://www.kaggle.com/datasets/chidozieuzoegwu/cvd-vital-signs, [Accessed 09-04-2024].

[55] H. L. Chidozie Louis Uzoegwu Farah Ahmed, *Ijsr.net*, https://www.ijsr.net/archive/v12i8/SR23809044938.pdf, [Accessed 09-04-2024], 2023.

[56] *MIMIC-III Clinical Database v1.4 — physionet.org*, https://physionet.org/content/mimiciii/1.4/, [Accessed 09-04-2024].

[57] T. Shimazui, T.-a. Nakada, K. R. Walley, T. Oshima, T. Abe, H. Ogura, A. Shiraishi, S. Kushimoto, D. Saitoh, S. Fujishima, *et al.*, "Significance of body temperature in elderly patients with sepsis", *Critical care*, vol. 24, pp. 1–9, 2020.

[58] S. Forsström and U. Jennehag, "A performance and cost evaluation of combining opc-ua and microsoft azure iot hub into an industrial internet-of-things system", in *2017 Global Internet of Things Summit (GIoTS)*, IEEE, Geneva, Switzerland, 2017, pp. 1–6.

[59] N. Abouzakhar and A. Bakar, "A chi-square testing-based intrusion detection model", in *Procs 4th International Conference on Cybercrime Forensics Education & Training*, Canterbury, United Kingdom, 2010.

[60] K. Cresswell, A. Domínguez Hernández, R. Williams, and A. Sheikh, "Key challenges and opportunities for cloud technology in health care: Semistructured interview study", *JMIR Hum Factors*, vol. 9, no. 1, e31246, Jan. 2022, ISSN: 2292-9495. DOI: 10.2196/31246. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/34989688.

[61] L. A. Jawad, "Security and privacy in digital healthcare systems: Challenges and mitigation strategies", *Abhigyan*, vol. 42, no. 1, pp. 23–31, 2024.

[62] S. Pearson, "Privacy, security and trust in cloud computing", in *Privacy and Security for Cloud Computing*, S. Pearson and G. Yee, Eds. London: Springer London, 2013, pp. 3–42. DOI: 10.1007/978-1-4471-4189-1_1.

[63] M. Kumar, *Optimizing Security for Remote Patient Monitoring with Edge Computing Strategies | International Research Journal on Advanced Engineering and Management (IRJAEM) — doi.org*, https://doi.org/10.47392/IRJAEM.2024.0207, [Accessed 26-07-2024].

[64] D. M. Botín-Sanabria, A.-S. Mihaita, R. E. Peimbert-García, M. A. Ramírez-Moreno, R. A. Ramírez-Mendoza, and J. d. J. Lozoya-Santos, *Digital Twin Technology Challenges and Applications: A Comprehensive Review — doi.org*, https://doi.org/10.3390/rs14061335, [Accessed 26-07-2024].