Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2018) 000–000

Procedia
Computer Science

www.elsevier.com/locate/procedia

A Cloud-based Secure Architecture for Remote Patient Monitoring Integrating OPC UA and Human Digital Twin

Jolly Trivedi[a], Jouni Isoaho[a], Tahir Mohammad[a]

[a]*Department of Computing, University of Turku, Turku 20014, Finland*

Abstract

Integrating Human Digital Twin (HDT) technology into Remote Patient Monitoring (RPM) systems represents a transformative advancement in personalized healthcare, addressing critical challenges related to data security and patient privacy. This paper presents a secure architectural framework designed to enhance personalized healthcare delivery in RPM by seamlessly combining wearable healthcare devices with the OPC Unified Architecture (OPC UA) protocol. Pseudonymization techniques are employed in the proposed architecture to establish a multi-layered security strategy that effectively protects sensitive patient data while preserving its usefulness for personalized healthcare. Data is securely transported to the cloud using Azure IoT Hub, resulting in a reliable pipeline for critical health information. The culmination of the architecture is Azure Digital Twin, which uses real-time patient data to enable customized healthcare interventions using predictive modeling and advanced analytics. By adhering to NIST SP 1800-30B criteria, the proposed system not only ensures compliance with regulatory standards but also provides a framework capable of adapting to emerging cybersecurity threats. The proposed architecture demonstrates performs better compared to existing RPM systems validated through comprehensive testing, including statistical analyses such as Chi-Square studies. Ultimately, this paper outlines a roadmap for the future of secure, personalized remote patient care, emphasizing the need for further investigation and pilot testing to validate the system's scalability and real-world applicability.

Keywords: Remote Patient Monitoring; RPM; Human Digital Twin; Pseudonymization; HDT; Security; Privacy; Cloud; HIPAA; GDPR; Healthcare

1. Introduction

The introduction of RPM systems, which enable real-time patient monitoring and management outside of conventional clinical settings, represents a revolutionary change in the healthcare industry. These systems typically utilize wearable devices to collect health data, which is then transmitted to the cloud for analysis and storage. Despite the benefits, using cloud-based platforms involves serious security concerns, such as data breaches, illegal access, and data integrity threats. Remote patient monitoring (RPM) offers significant clinical benefits but raises important security and privacy concerns. The transmission of electronic health records (EHR) in RPM systems requires robust security

* Corresponding author.

measures to protect sensitive patient data [1]. Privacy and data security considerations are crucial for maintaining patient confidence and addressing ethical and legal risks [2]. Key challenges include ensuring the confidentiality, integrity, and availability of health data during collection, transfer, and storage [3]. Transport Layer Security (TLS) protocols have been used to address these issues [1]. Ongoing research and development in this area are necessary to mitigate evolving cybersecurity risks in RPM ecosystems. The implementation of comprehensive security and privacy measures is essential for the successful deployment and social acceptance of RPM technologies [5]. Additionally, enforcing privacy through security measures and practices is essential to protect patient confidentiality and maintain trust in these systems [6]. Balancing clinical utility with privacy and security requirements remains a critical challenge in the development and adoption of RPM systems [2]. The National Cybersecurity Center of Excellence (NCCoE) warns that the growing usage of telehealth and RPM systems makes them vulnerable to hackers, highlighting the need for strong security measures. The proposed architecture aims to create a secure and effective future for healthcare delivery.

1.1. Motivation

Despite the potential benefits of integrating OPC UA and HDT with RPM systems, there is insufficient data to evaluate how successfully these linkages enhance data security as well as personalized healthcare. The majority of existing research focuses on theoretical aspects of these technologies or provides minimal empirical evidence of their real-world implementation [7]. This study proposes and evaluates a cloud-based secure architecture for RPM that makes use of OPC UA and HDTs. The proposed architecture includes strong security mechanisms, including pseudonymization and encryption, to secure patient data during transmission and storage. The integration of HDTs allows for individualized healthcare interventions by giving tailored insights based on real-time data [8]. This research aims to give empirical evidence of the benefits of integrating OPC UA and HDTs in terms of data security and customized healthcare by comparing the proposed architecture to existing RPM systems. The findings of this study can help shape the development of future RPM systems and add to the expanding body of knowledge in the field of healthcare technology.

1.2. Contribution

The proposed architecture makes several significant contributions to the field of RPM systems.

1. **Proposed a Novel Architecture for Secure RPM Systems**: An innovative architecture specifically designed for remote patient monitoring (RPM) systems is introduced. The architecture integrates OPC UA, Azure IoT Hub, and Azure Digital Twin to create a secure, scalable, and efficient framework for handling patient data. The proposed architecture employs pseudonymization techniques to enhance patient data privacy. A comparative analysis between the proposed architecture and existing RPM systems is highlighted through Chi-Square analysis in terms of security, scalability, and personalization while also discussing its limitations.
2. **Integration of OPC UA and Azure Cloud Components**: The paper details the use of OPC UA as a key component in the architecture, providing standardized data communication with built-in security features such as encryption, authentication, and authorization. There are considerable advantages of integrating OPC UA and HDTs into RPM systems [9]. Azure IoT Hub acts as the central hub between OPCA UA and Azure Digital Twin that creates virtual models (HDT) of patient health profiles to enable advanced analytics, real-time monitoring, and predictive modeling, leading to more personalized and effective patient care. This integration enables healthcare practitioners to provide individualized therapies, which increases patient involvement and adherence to treatment programs [10].

1.3. Organization of paper

The rest of paper is organized as follows: Section 2 provides the background of the core technologies considered for the proposed architecture. Section 3 describes the work done related to remote patient monitoring systems. Section 4 presents the proposed architecture - SecureHealth and explains the data flow. Section 5 describes the Design and Implementation of the SecureHealth. Section 6 provides details about the statistical analysis and the results. The next section lists the limitations of SecureHealth followed by the direction of Future Work. The paper concludes with an overall summary of the research work.

2. Background

2.1. IoMT (Internet Of Medical Things)

IoMT enables the seamless integration of various medical devices, sensors, and wearables into the RPM system. This interconnected network allows for continuous and real-time data collection from patients, providing healthcare providers with up-to-date and accurate health metrics. IoMT's potential extends to cardiovascular health monitoring, fall prediction, and ensuring real-time security in remote patient monitoring through lightweight cryptography [12].

2.2. OPC UA (Open Platform Communications Unified Architecture)

OPC UA facilitates secure and reliable data exchange between devices and systems, making it an ideal choice for integrating diverse healthcare technologies. Key features of OPC UA include interoperability, security, and scalability. OPC UA is emerging as a promising framework for integrating heterogeneous healthcare systems and enabling Industry 4.0 compliance in the healthcare sector [13]. In healthcare specifically, OPC UA can be used to develop data models based on the HL7 Reference Information Model for information exchange and storage [13].

2.3. HDT (Human Digital Twin)

HDTs offer significant benefits for RPM systems in healthcare. HDTs provide real-time monitoring and decision support, enabling medical staff to determine optimal treatments [15]. They can accurately represent an individual's molecular, physiological, emotional, and lifestyle status, facilitating personalized healthcare applications [16]. Human Digital Twins harness diverse data to assess health and provide insights to individuals and medical facilities. These assessments yield predictions, advice, and alerts for the individual and their healthcare providers. These insights prompt lifestyle adjustments or medical interventions. In critical situations, the system can trigger immediate emergency responses, including dispatching ambulances and initiating urgent care protocols [14]. HDTs show great potential for improving RPM and personalized healthcare as they enable real-time monitoring and personalized healthcare [15].

3. Related Work

In recent years, there has been increased interest in integrating Human Digital Twin (HDT) technology into Remote Patient Monitoring (RPM) systems. However, the available research does not provide a complete approach to protecting patient data while maximizing the benefits of HDT and OPC UA in RPM systems. Several studies have explored various aspects of RPM systems, particularly focusing on enhancing security measures, ensuring data privacy, and improving interoperability across different healthcare devices. Despite these efforts, gaps remain in fully addressing these critical challenges, particularly in integrating advanced security protocols and leveraging modern cloud technologies for enhanced personalization and analytics.

Most of the existing systems do not fully leverage modern cloud-based platforms, which offer more advanced security features and scalability. This encouraged to implementation of Azure IoT Hub and Azure Digital Twin in the proposed architecture. Key concerns include protecting patient data from unauthorized access and ensuring proper user identification in multi-user environments [4]. To address these issues, the proposed architecture implements pseudonymization over the health data received. This ensures robust data security and privacy. Pseudonymization has emerged as a more balanced approach, allowing the data to retain its analytical value while protecting patient identities. Nevertheless, there is a notable lack of comprehensive frameworks that integrate pseudonymization with advanced security protocols in cloud-based RPM systems.

Interoperability remains a significant challenge in the deployment of RPM systems. While some studies have explored the use of standardized protocols like HL7 and FHIR for data exchange in healthcare systems, these protocols are often not specifically designed for IoT-based RPM systems. OPC UA (Open Platform Communications Unified

Architecture) has been recognized as a potential solution due to its interoperability, security, and scalability features. However, its application in RPM systems is still relatively underexplored, particularly in conjunction with modern cloud services like Azure IoT Hub and Azure Digital Twin, which offer powerful tools for data analysis, predictive modeling, and personalized healthcare. Elkhodr et al. [1] aims to emphasize the importance of securing the transmission of Electronic Health Records (EHR) of patients in remote health monitoring systems by proposing solutions built on Transport Layer Security (TLS) protocols. Most of the existing work focuses on the Network layer but the proposed architecture focuses on the Communication Layer mainly and then on the Cloud Layer. The proposed architecture is better aligned with relevant regulations and standards compared to the IoT-based heart monitoring system [18] and the real-time heart monitoring system [19] using smartphone and wearable sensors.

4. Proposed architecture - SecureHealth

The proposed architecture for the Remote Patient Monitoring (RPM) system displayed in Fig. 1 for enhancing security in RPM systems. The architecture is composed of several key components, each playing a critical role in ensuring the secure and efficient operation of the RPM system. As a substitute for real-world healthcare devices, an OPC UA simulation server is used to generate and transmit patient data similar to wearable device data. This simulation allows for the testing and validation of the architecture in a controlled environment while replicating the functionality of actual wearable devices. This cloud-based platform acts as the central gateway for securely transmitting data from the OPC UA server to the cloud. Azure IoT Hub provides features such as device authentication, secure messaging, and device management, ensuring that data is securely routed to the appropriate cloud services. Before transmitting data to the cloud, the architecture applies encryption and pseudonymization techniques. Encryption protects data integrity during transmission, while pseudonymization replaces identifiable patient information with pseudonyms, ensuring privacy and compliance with regulations like HIPAA and GDPR. Azure Digital Twin creates a Human Digital Twin of patients based on the incoming data. HDT are used for real-time monitoring, advanced analytics, and predictive modeling, enabling personalized healthcare interventions.

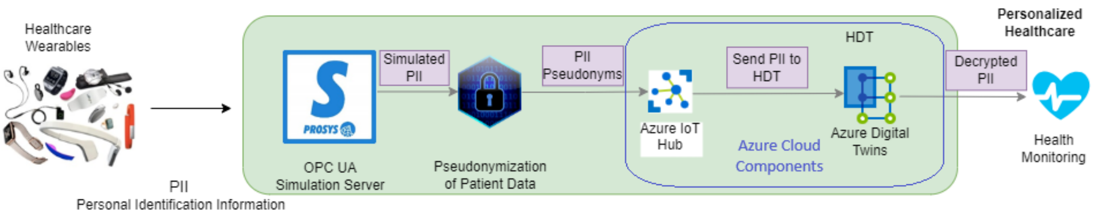


Fig. 1. The Proposed Architecture - SecureHealth

The proposed architecture is compliant to NIST, HIPAA and GDPR. This compliance simplifies regulatory oversight for healthcare providers, reducing the administrative burden associated with data management and ensuring adherence to legal requirements. Furthermore, the architecture incorporates multiple layers of security, including strong authentication, role-based access control, and secure data encryption, to protect against unauthorized access. By ensuring that only authorized users and devices can access sensitive information, the system minimizes the risk of data misuse. The architecture's emphasis on data integrity, security, and compliance provides a reliable foundation for the development and deployment of advanced RPM systems.

5. Design and Implementation

The Data Flow in SecureHEalth is explained in Fig 2. The data flow in the proposed architecture for securing remote patient monitoring (RPM) systems is meticulously designed to ensure the seamless, secure, and efficient transmission of patient data from wearable devices to the cloud, where it is stored, analyzed, and utilized for real-time monitoring and predictive healthcare.

The first step in the implementation is the configuration of the OPC UA simulation server. This server is programmed to simulate the data such as heart rate and temperature of the patient. The simulated data is periodically

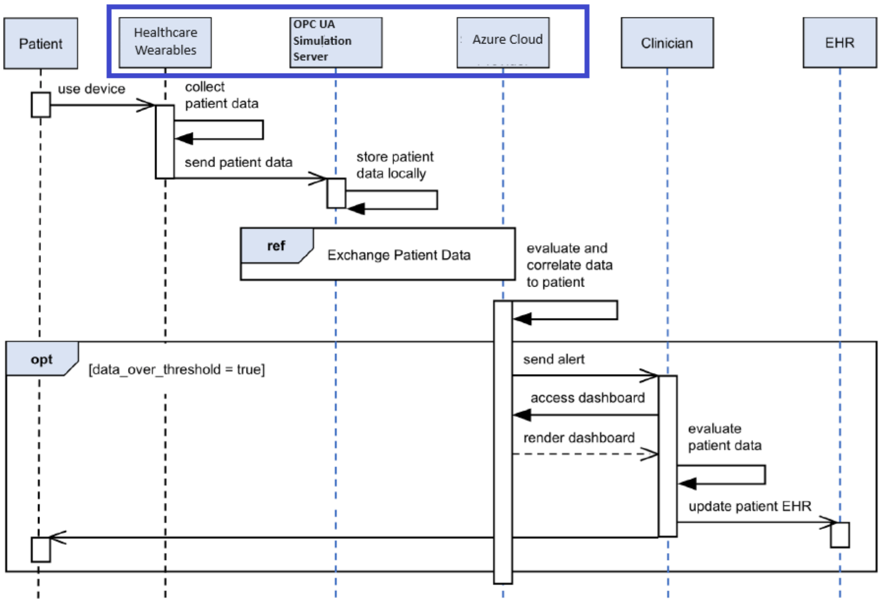


Fig. 2. Algorithm: Chi-Square Test for Comparing RPM Systems

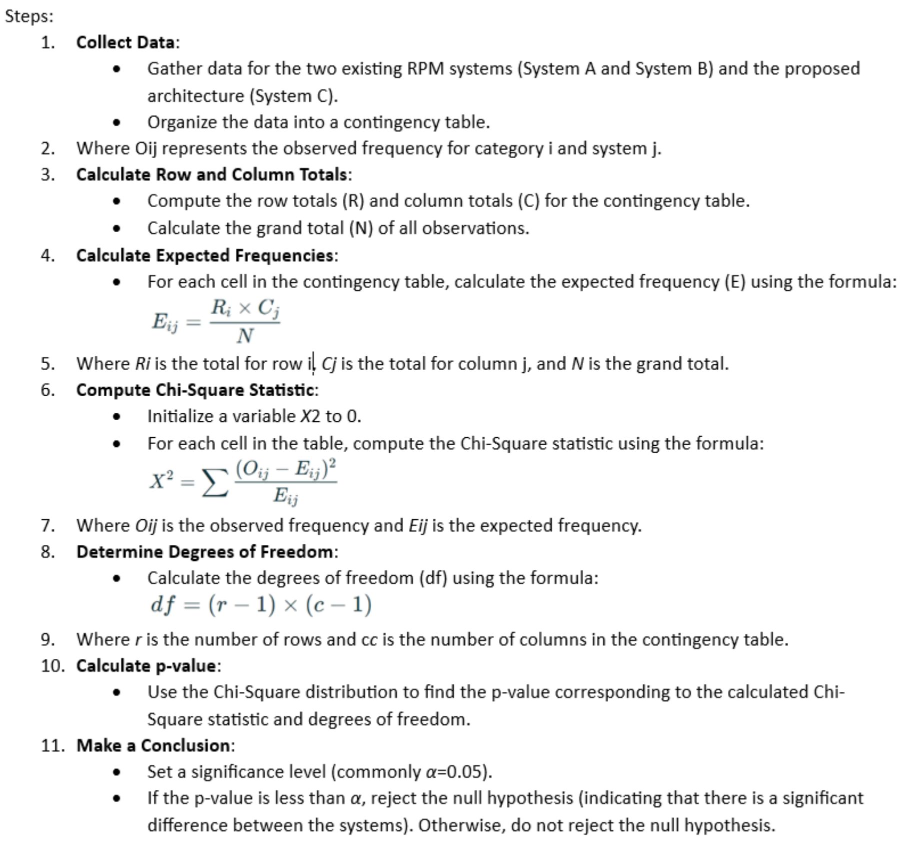
updated and sent through the OPC UA protocol. Azure IoT Hub is configured to receive data from the OPC UA server. This involves setting up the necessary device identities and authentication mechanisms to ensure that only authorized devices can send data. The IoT Hub is also configured to manage the secure routing of data to subsequent components of the architecture. Before the data is transmitted to the cloud, encryption algorithms are applied to protect data during transmission. Pseudonymization techniques are then used to replace any identifiable information within the data payload with unique pseudonyms. This step ensures that patient identities are protected and that the data is compliant with privacy regulations. The encrypted and pseudonymized data is then sent to Azure Digital Twin. Here, the data is used to update the virtual models of patients. The Digital Twin environment is configured to process incoming data in real-time, allowing for the continuous monitoring of patient health and the generation of predictive insights. Finally, the data, once analyzed, is securely stored in Azure cloud storage. Analytics services are configured to perform further analysis on the stored data, providing healthcare providers with actionable insights and enabling personalized patient care plans.

After the architecture is fully implemented, the code written to transmit the data is tested in the Visual Studio Community version on Windows OS and using Visual Studio Code IDE on the Ubuntu OS. It is tested on multiple operating systems to evaluate its performance by calculating the maximum response time. Security analysis was done through Chi-Square analysis.

6. Test and Performance Analysis

This section presents the results of the statistical analysis conducted to assess the effectiveness of the proposed cloud-based secure architecture for Remote Patient Monitoring (RPM) systems. The evaluation utilized a Chi-Square test to compare the performance of the proposed architecture against two existing RPM systems. The analysis focused on key performance metrics, including Data Encryption, Access Controls, Secure Data Transfer, Data Privacy, Regulatory Compliance, Cloud Security, and Audit Logging.

Data for the evaluation was collected from three RPM systems: the proposed architecture - SecureHealth, IoT based Heart rate monitoring [18] and A Real-Time Health Monitoring System for Remote Cardiac Patients Using Smartphone and Wearable Sensors [19]. The Chi-Square test was employed to determine whether there were statistically significant differences in the performance metrics among the three systems. The algorithm for the test is displayed in Fig. 3. The findings from the Chi-Square test revealed that the proposed architecture - SecureHealth demonstrated a significant reduction in security incidents compared to the existing systems [18] [19]. The Chi-Square test results affirm the effectiveness of the proposed cloud-based secure architecture for RPM systems. The significant differences observed in performance metrics highlight the advantages of integrating OPC UA and HDTs, paving the way for enhanced patient care and improved health outcomes. Future research may explore additional performance metrics and long-term impacts to further validate the benefits of the proposed architecture.



Steps:

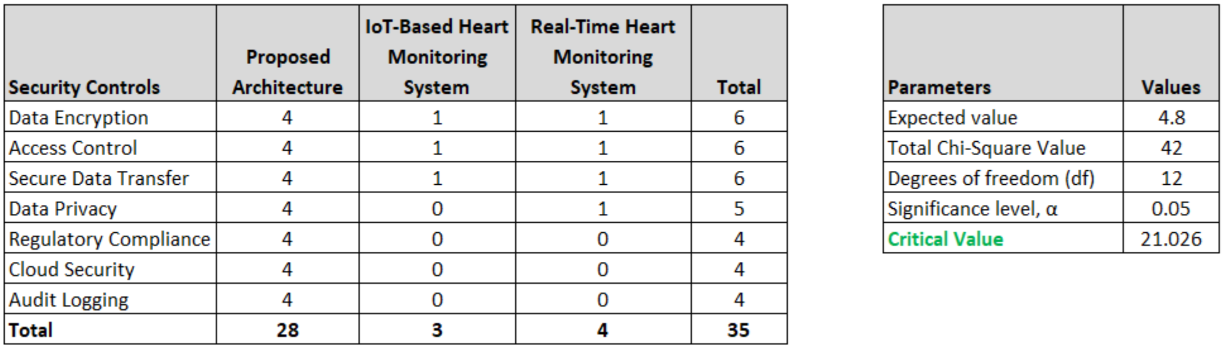
1. **Collect Data**:
   - Gather data for the two existing RPM systems (System A and System B) and the proposed architecture (System C).
   - Organize the data into a contingency table.
2. Where Oij represents the observed frequency for category i and system j.
3. **Calculate Row and Column Totals**:
   - Compute the row totals (R) and column totals (C) for the contingency table.
   - Calculate the grand total (N) of all observations.
4. **Calculate Expected Frequencies**:
   - For each cell in the contingency table, calculate the expected frequency (E) using the formula:

     $$E_{ij} = \frac{R_i \times C_j}{N}$$
5. Where *Ri* is the total for row i, *Cj* is the total for column j, and *N* is the grand total.
6. **Compute Chi-Square Statistic**:
   - Initialize a variable *X*2 to 0.
   - For each cell in the table, compute the Chi-Square statistic using the formula:

     $$X^2 = \sum \frac{(O_{ij} - E_{ij})^2}{E_{ij}}$$
7. Where *Oij* is the observed frequency and *Eij* is the expected frequency.
8. **Determine Degrees of Freedom**:
   - Calculate the degrees of freedom (df) using the formula:

     $$df = (r - 1) \times (c - 1)$$
9. Where *r* is the number of rows and *c*c is the number of columns in the contingency table.
10. **Calculate p-value**:
    - Use the Chi-Square distribution to find the p-value corresponding to the calculated Chi-Square statistic and degrees of freedom.
11. **Make a Conclusion**:
    - Set a significance level (commonly α=0.05).
    - If the p-value is less than α, reject the null hypothesis (indicating that there is a significant difference between the systems). Otherwise, do not reject the null hypothesis.

Fig. 3. Algorithm: Chi-Square Test for Comparing RPM Systems



Security Controls	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**

(a)

Parameters	Values
Expected value	4.8
Total Chi-Square Value	42
Degrees of freedom (df)	12
Significance level, α	0.05
Critical Value	21.026

(b)

Fig. 4. Contigency Table and Results of Chi-Square Test Comparing RPM Systems

The unique security controls were first identified from considered sources for the Chi-Square test. The contingency table displayed in Fig 4(a) was created to compare security controls between the proposed architecture and existing works of literature. The frequency of each security control mentioned in the proposed architecture and the literature was then counted and recorded in the appropriate cells of the contingency table. The results of the test are displayed in Fig 4(b). As mentioned in Fig 4(b), the calculated chi-square value (42.00) is greater than the critical value (21.026), which leads to the rejection of the null hypothesis. This indicates a significant difference in the frequencies of the security controls among the three systems. The results of this evaluation provide valuable insights into the advantages of the proposed approach and demonstrate its potential to enhance patient care.

7. Limitations & Future Directions

This study presents a robust architecture for secure and personalized remote patient monitoring (RPM) by integrating OPC UA with Azure IoT Hub and Azure Digital Twin. While the proposed solution offers significant improvements in data security, privacy, and system scalability, several limitations need to be addressed to enhance the feasibility and effectiveness of the system in real-world applications.

One significant limitation of this architecture is the complexity of implementation. The integration of multiple advanced technologies, such as OPC UA, Azure IoT Hub, and Azure Digital Twin, requires extensive expertise and resources. This high level of technical expertise required may limit the adoption of the proposed architecture, especially for smaller healthcare providers with limited technical resources and support infrastructure. Another limitation concerns the cost. The utilization of cloud services, particularly Azure IoT Hub and Azure Digital Twin, can incur significant operational costs. The financial burden associated with maintaining and operating cloud-based RPM systems may be a barrier to widespread adoption, particularly in resource-constrained settings or smaller healthcare facilities. Data sovereignty and compliance with regional regulations are additional challenges. Cloud-based solutions must adhere to data sovereignty laws, which require data to be stored and processed within specific geographical boundaries. Ensuring compliance with healthcare regulations such as HIPAA and GDPR further complicates the implementation process. Mismanagement of cloud security settings or inadequate protection measures can lead to data breaches or unauthorized access.

Addressing these challenges requires careful consideration of technical, economic, and regulatory factors to ensure successful implementation and widespread adoption. Future work should focus on optimizing the architecture to overcome these limitations and enhance the feasibility and effectiveness of RPM systems in various healthcare settings.

8. Conclusion

The proposed architecture in this paper addresses existing RPM challenges by integrating OPC UA for secure and standardized communication, pseudonymization for enhanced privacy, and Azure IoT Hub and Digital Twin for advanced data analysis and predictive modeling. This holistic approach aims to fill the critical gaps identified in current RPM systems, contributing to the advancement of secure, efficient, and personalized remote healthcare solutions. By addressing existing gaps in the literature, this work serves as a foundation for future research and development in the field of healthcare technology. The statistical analysis conducted in this study, utilizing a Chi-Square test, has provided valuable insights into the advantages of the proposed architecture. Looking ahead, the integration of OPC UA and HDTs into RPM systems presents numerous opportunities for further exploration. Investigating the scalability of the proposed architecture in real-world settings, exploring additional security protocols, and implementing federated learning are among the avenues for future research. As the field continues to evolve, embracing innovations like federated learning and edge computing will be essential in pushing the boundaries of what is possible in remote patient monitoring and improving patient outcomes.

References

[1] Elkhodr, Mahmoud and Shahrestani, Seyed and Cheung, Hon. (2011) ”Ubiquitous health monitoring systems: Addressing security concerns” *Journal of Computer Science* **7** (10): 1465

[2] Choi, Peter and Walker, Rachael. (2019) ”Remote patient management: Balancing patient privacy, data security, and clinical needs” *Remote patient management in peritoneal dialysis* **197** 35–43

[3] Pramanik, Pijush Kanti Dutta and Pareek, Gaurav and Nayyar, Anand. (2019) ”Security and privacy in remote healthcare: Issues, solutions, and standards” *Telemedicine technologies,Elsevier* 201–225

[4] Ondiege, Brian and Clarke, Malcolm and Mapp, Glenford. (2017) ”Exploring a new security framework for remote patient monitoring devices” *Computers, MDPI* **6** (1): 11

[5] Grayson, Nakia and Pulivarti, Ronald and Hodges, Bronwyn and Littlefield, Kevin and Miller, Jeremy and Peloquin, Chris and Snyder, Julie and Wang, Sue and Williams, Ryan. (2023) ”Mitigating Privacy and Cybersecurity Risks Affecting Telehealth Remote Patient Monitoring Ecosystems” *Computer, IEEE* **56** (9): 50–61.

[6] Raman, Abhay. (2007) ”Enforcing privacy through security in remote patient monitoring ecosystems” *2007 6th International Special Topic Conference on Information Technology Applications in Biomedicine, IEEE* 298–301

[7] Hamine, Saee and Gerth-Guyette, Emily and Faulx, Dunia and Green, Beverly B and Ginsburg, Amy Sarah. (2015) ”Impact of mHealth Chronic Disease Management on Treatment Adherence and Patient Outcomes: A Systematic Review” *Journal of Medical Internet Research* **17**(2):e52

[8] Bodenheimer, Thomas and Sinsky, Christine. (2014) ”From triple to quadruple aim: care of the patient requires care of the provider” *The Annals of Family Medicine* **12**(6):573–576

[9] Jiang, Fei and Jiang, Yong and Zhi, Hui and Dong, Yi and Li, Hao and Ma, Sufeng and Wang, Yilong and Dong, Qiang and Shen, Haipeng and Wang, Yongjun. (2017) ”Artificial intelligence in healthcare: past, present and future” *Stroke and vascular neurology* **2**(4)

[10] Kruse, Clemens Scott and Kothman, Krysta and Anerobi, Keshia and Abanaka, Lillian. (2016) ”Adoption factors of the electronic health record: a systematic review” *JMIR medical informatics* **4**(2): e5525

[11] Nishad, Dipesh Kumar and Tripathi, Diwakar R. (2020) ”Internet of Medical Things (IoMT): Applications and Challenges” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* **11** (3): 2885–2889

[12] ”A Survey on Transforming Healthcare with IoMT : The Power of Connected Medical Devices” Dr. D. Antony Arul Raj Arul Raj, Dr. K. V. Rukmani, Subiksha S Rukmani, Vimal P Rukmani, Deepak Kumar K. (2024) *International Journal of Scientific Research in Computer Science Engineering and Information Technology***10**:(2)

[13] Miranda, Jorge and Cabral, Jorge and Banerjee, Suprateek and Grossmann, Daniel and Pedersen, Christian F and Wagner, Stefan R. (2017) ”Analysis of OPC unified architecture for healthcare applications” *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus* 1–4

[14] Wei Shengli. (2021) “Is Human Digital Twin possible?” *Computer Methods and Programs in Biomedicine Update* **1**

[15] Sirigu, Giorgia and Carminati, Barbara and Ferrari, Elena. (2022) ”Privacy and security issues for human digital twins” *2022 IEEE 4th international conference on trust, privacy and security in intelligent systems, and applications (TPS-ISA)* 1–9

[16] Chen, Jiayuan and Yi, Changyan and Okegbile, Samuel D and Cai, Jun and Shen, Xuemin Sherman. (2023) ”Networking architecture and key supporting technologies for human digital twin in personalized healthcare: a comprehensive survey” *IEEE Communications Surveys & Tutorials*

[17] Khan, Sangeen and Ullah, Sehat and Khan, Habib Ullah and Rehman, Inam Ur. (2023) ”Digital-Twins-Based Internet of Robotic Things for Remote Health Monitoring of COVID-19 Patients” *IEEE Internet of Things Journal* **10** (18):16087–16098

[18] Umer, Muhammad and Aljrees, Turki and Karamti, Hanen and Ishaq, Abid and Alsubai, Shtwai and Omar, Marwan and Bashir, Ali Kashif and Ashraf, Imran. (2024) ”Heart failure patients monitoring using IoT-based remote monitoring system - Scientific Reports — nature.com” *Nature.con*

[19] Kakria, Priyanka and Tripathi, Nitin and Kitipawong, Peerapong. (2015) ”A Real-Time Health Monitoring System for Remote Cardiac Patients Using Smartphone and Wearable Sensors” *International Journal of Telemedicine and Applications* 1-11