Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 251 (2024) 248–255

Procedia Computer Science

www.elsevier.com/locate/procedia

The 15th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2024)
October 28-30, 2024, Leuven, Belgium

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

This paper suggests a secure architecture for Remote Patient Monitoring (RPM) systems that integrate Azure IoT Hub, Azure Digital Twin, and OPC UA in order to enhance the security of patient data, data privacy, and personalized healthcare services. RPM systems track real-time health data of patients through wearable devices. In this process, they face significant security challenges specifically related to data encryption, access control, and compliance with the security requirements of regulations like HIPAA and GDPR. To overcome these concerns, the proposed architecture in the paper utilizes OPC UA for secure and compliant communication between healthcare devices and the cloud. An additional level of security is provided by the implementation of pseudonymization. Moreover, the personally identifiable information (PII) of the patient is removed before transferring to the cloud and hence assures compliance. Azure IoT Hub makes encrypted data flow in the cloud which is then transferred to Human Digital Twin (HDT) for real-time analysis and enhancing personalized healthcare. The integration of multiple layers of security, including role-based access control (RBAC) and encryption, in the architecture protects against data breaches and unauthorized access. The suggested architecture provides adequate security features compared to existing RPM systems, as indicated by statistical analysis using the Chi-Square test. This test was performed for security metrics like Data Encryption, Access Controls, Secure Data Transfer, Data Privacy, Regulatory Compliance, Cloud Security, and Audit Logging.

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

1. Introduction

Healthcare has undergone under major shift with the development of RPM systems that enable real-time patient monitoring and management outside of conventional clinical settings. RPM systems collect data using wearable de-

* Corresponding author.
E-mail address: tahir.mohammad@utu.fi

10.1016/j.procs.2024.11.107

vices, which is then transmitted to the cloud for analysis and storage. However, there are certain security challenges to utilizing cloud-based platforms, like data breaches, illegal access, and data integrity threats, although they offer significant clinical benefits. Adequate security measures are required for the distribution of Electronic Health Records (EHR) to protect the sensitive data of patients [1]. Privacy and data security considerations are very important for maintaining patient confidence and addressing ethical and legal risks [2]. During the process of collection, transfer, and storage, it is challenging to maintain confidentiality, integrity, and availability [3]. In one of the works, 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]. Moreover, to ensure the protection of patient confidentiality and maintain trust in RPM systems, it is necessary to enforce security and privacy [6]. Another challenge encountered with the advancement of RPM systems is balancing clinical utility with security requirements and privacy [2]. The warning has been given by the National Cybersecurity Center of Excellence (NCCoE) regarding telehealth and RPM systems being vulnerable to attacks due to their growing usage, highlighting the need for strong security measures. The proposed architecture lays a foundation for 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 integrates OPC UA and HDTs. The need for enhanced data privacy and security motivated to implementation of pseudonymization logic. The integration of HDTs allows for individualized healthcare interventions by giving tailored insights based on real-time data [8]. This research discussed the role of 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 architectural design specifically tailored for RPM systems is presented. The architecture integrates OPC UA, Azure IoT Hub, and Azure Digital Twin (ADT) to create a secure, scalable, and efficient framework for handling patient data. The incorporation of OPC UA provides a secure and standardized method for communication between healthcare wearable devices and the cloud, thus addressing the challenge of confidentiality and data integrity in RPM systems. 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. **Secure and Personalised RPM with HDT**: ADT in the architecture enables the implementation of HDT technology. HDT processes the real-time data of patients and updates the virtual model, which helps in making decisions and early diagnosis of chronic diseases, leading to the enhancement of personalized healthcare. HDT can integrate data from multiple devices and patients and manage their digital replicas without increasing the load on conventional healthcare infrastructures. Traditional RPM systems majorly rely on the data collected periodically which can result in delayed responses in critical conditions. HDT technology overcomes this challenge by continuously monitoring and providing a secure and timely detection system. Creating HDT through ADT enhances the security of this functionality through encryption and role-based access control(RBAC) for authorized access to the virtual data of the patient.

1.3. Organization of paper

The rest of the 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 RPM 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. Section 7 lists the limitations of SecureHealth, followed by the direction of Future Work. Finally, the conclusion is presented in Section 8.

2. Background

2.1. Internet Of Medical Things (IoMT)

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 RPM through lightweight cryptography [12].

2.2. Open Platform Communications Unified Architecture (OPC UA)

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. Human Digital Twin (HDT)

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]. HDTs 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. 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 HDT technology into 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 security measures, scalability, personalization, and analytics. Security and Privacy are the needs of Smart Healthcare as more and more cutting technologies are implemented to enhance patient care. REST API and MQTT are a few of the communication protocols currently used for security in RPM systems [21]. To address the shortcomings of these protocols, OPC UA has been experimented with in the proposed architecture considering its elevated security features.

This led to the utilizing Azure IoT Hub and Azure Digital Twins (ADT) within the proposed architectural framework. 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. z Interoperability remains a significant challenge in the deployment of RPM systems. A novel open architecture for the patient has been developed and implemented, which features the integration of RPM systems into Hospital Information Systems (HIS) with an interface for standardized communication to achieve effective real-time monitoring and data processing [20]. 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 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 ADT, 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 EHR of patients in remote health monitoring systems by proposing solutions built on 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 RPM system is shown 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 replicates the functionality of actual wearable devices and allows the testing and validation of the architecture in a controlled environment. The data is transmitted securely from the OPC UA server to the cloud through his platform. Azure IoT Hub provides features such as device authentication, device management, and secure messaging, 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. HDT of patients based on the incoming data is created using ADT. HDT are used for real-time monitoring, advanced analytics, and predictive modeling, enabling personalized healthcare interventions.

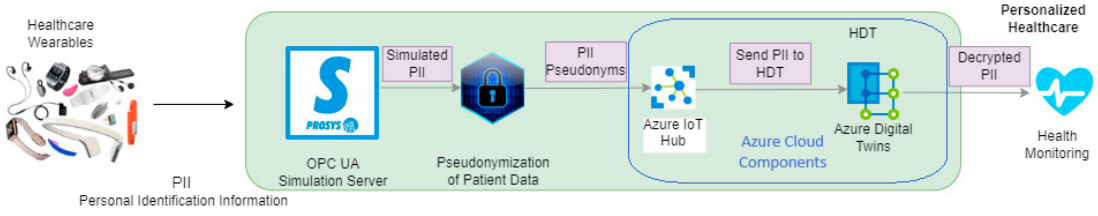

Fig. 1. The Proposed Architecture - SecureHealth

The proposed architecture is compliant with NIST, HIPAA, and GDPR from a security perspective. 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 presented in Fig 2. is 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.

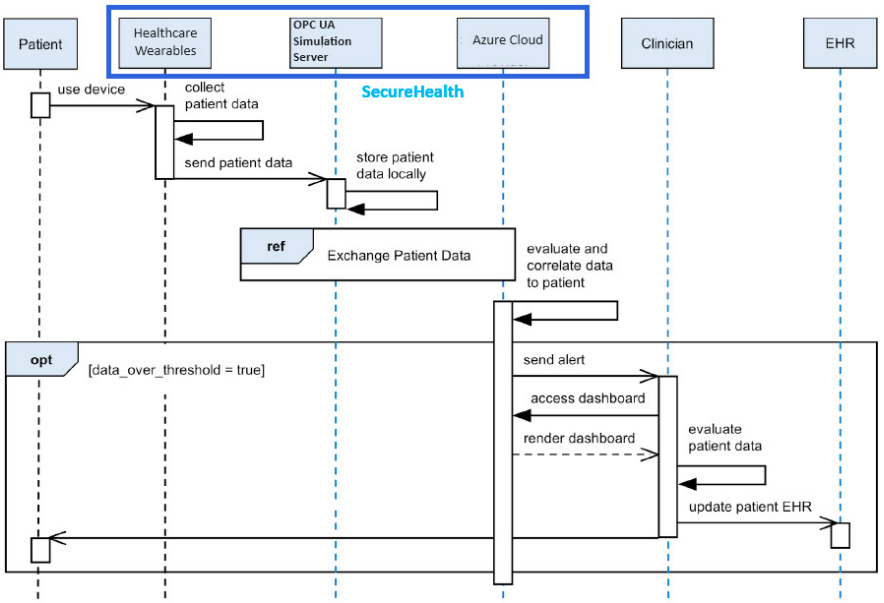

Fig. 2. Algorithm: DataFlow Diagram for proposed SecureHealth

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 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 as it is an ideal choice for comparing the security metrics of the systems. This test is also ideal for analyzing the system performance of the existing RPM systems for varied populations of patients which can be considered in future work.

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 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. These security metrics are categorical and the Chi-Square test helps in analyzing the significant association between these security measures and the incidents captured by RPM systems.

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.

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 *cc* 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

The unique security controls were first identified from considered sources for the Chi-Square test. The contingency table displayed in Fig 4(a) compares security controls between the proposed architecture and existing works of literature. In the table, the count shows the number of controls in the RPM system that meet the security objective defined by the metric. The results of the test are displayed in Fig 4(b), calculated based on the algorithm in Figure 3. As

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

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 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 paper proposes SecureHealth architectural framework that integrates OPC UA for secure and standardized communication, pseudonymization for enhanced privacy, and Azure IoT Hub and Digital Twin for secure and advanced data analysis and predictive modeling. SecureHealth addresses the crucial challenges identified in current RPM systems, contributing to the advancement of secure, efficient, and personalized remote healthcare solutions. By

identifying and addressing challenges in securing RPM systems, this work serves as a foundation for future research and development in the field of healthcare technology. The statistical analysis done during this research utilizing a Chi-Square test, has provided valuable insights into the advantages of the suggested architectural framework. 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 there are advancements in RPM systems, integration of federated learning can help forecast the anomalies better as well as enhance data privacy. It is the need of time to embrace advances in Artificial Intelligence and Edge Computing to expand the capabilities of RPM systems and consequently improve patient well-being.

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] D. Antony Arul Raj, Arul Raj, K. V. Rukmani, Subiksha S Rukmani, Vimal P Rukmani, Deepak Kumar K. (2024). A Survey on Transforming Healthcare with IoMT : The Power of Connected Medical Devices" *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

[20] Varady, P. and Benyo, Z. and Benyo, B. (2002) "An open architecture patient monitoring system using standard technologies" *IEEE Transactions on Information Technology in Biomedicine* **6**(1): 95-98

[21] Chia-Rong Su and Jeyhun Hajiyev and Changjui James Fu and Kuo-Chin Kao and Chih-Hao Chang and Ching-Ter Chang (2019) A novel framework for a remote patient monitoring (RPM) system with abnormality detection" *Health Policy and Technology* **8**(2): 157-170