Secure and Resilient Framework for Internet of Medical Things (IoMT) with an Effective Cybersecurity Risk Management

[1]**Latifah Khalid Alabdulwahhab and** [2]**Shaik Shakeel Ahamad**

[1&2]Department of Information Technology, College of Computer and Information Sciences Majmaah University, Al-Majmaah, 11952, Saudi Arabia

Summary
COVID-19 pandemic outbreak increased the use of Internet of Medical Things (IoMT), but the existing IoMT solutions are not free from attacks. This paper proposes a secure and resilient framework for IoMT, it computes the risk using Risk Impact Parameters (RIP) and Risk is also calculated based upon the Threat Events in the Internet of Medical Things (IoMT). UICC (Universal Integrated Circuit Card) and TPM (Trusted Platform Module) are used to ensure security in IoMT. PILAR Risk Management Tool is used to perform qualitative and quantitative risk analysis. It is designed to support the risk management process along long periods, providing incremental analysis as the safeguards improve.

Keywords:
Internet of Medical Things (IoMT); Risk Management; PILAR Risk Management Tool; Risk Impact Parameters (RIP), UICC (Universal Integrated Circuit Card); TPM (Trusted Platform Module)

1. Background

The enormous development in the realm of information and communication technology infrastructure played pivotal role in providing good solutions in healthcare, payments and mobile commerce. Internet of Medical Things (IoMT) delivers healthcare services anywhere at any time which is a boon for the patients. Mobile devices, hospital servers, healthcare applications in mobile devices and computer networks plays vital role in providing healthcare services to the patients at home. Mobile devices, hospital servers, healthcare applications in mobile devices and computer networks are the main target of intruders so security and privacy are very important for the successful implementation and adoption of these services. Internet of Medical Things (IoMT) played crucial role during COVID-19 pandemic in providing services to patients at home, so Mobile Healthcare Applications (MHAs) plays vital role in the successful implementation of healthcare solutions. Attackers attack Mobile Healthcare Applications, networks and hospital servers, so the Healthcare service providers need to ensure security at the Applications, networks and hospital servers levels. Security and privacy are needed in healthcare services in order to ensure accuracy and efficiency. Security should be made a part of product right from the design phase, so that the healthcare solutions should be able to withstand any type of attack. In order to overcome the attacks on healthcare solution providers needs to do risk management. Risk Management is divided into Risk and Trust. Risk in IoMT is divided into Device Level Risk, Network level Risk and Storage and Processing Level Risk. Device Level Risk is at the Mobile Phone, UICC, Trusted Platform, Module (TPM) Server at the hospital. Network level Risk is at the network level there will be communication threats and vulnerabilities. Storage and Processing Level Risk is at the server side which is used to for the storage and processing of patient's data. Risk is assessed in two ways, they are Qualitative Assessment and Quantitative Assessment. Qualitative Assessment uses non-numerical based methods to identify and analyze the risk event. It considers descriptive measures in order to analyze the probability of risk recurring, so the probability is measured in high, low and moderate. Risk is assessed as Qualitative Assessment and Quantitative Assessment, Qualitative Assessment uses non-numerical methods in order to identify and analyze the risk event with their impact. In qualitative Assessment the probability is measured using a relative scale based on the terms such as low, moderate and high.

This method of risk assessment involves a subjective measure of estimation and is easy to perform. However, it is less accurate than the quantitative risk assessment. Quantitative risk assessment uses numerical values with a margin of error in order to pick and analyze the risk events and their impact whenever it occurs. This method uses deterministic, stochastic, and systematic approach. The results and values are expressed in numerical figures. PILAR Risk Management Tool is a tool used to perform

Manuscript received May 5, 2024
Manuscript revised May 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.5.8

qualitative and quantitative risk analysis. This assessment process supports for long periods and provides incremental analysis. Security and privacy are very challenging for mobile healthcare because of the patient's sensitive data. Many research works have highlighted the security challenges in the realm of IoMT (D.N. Burrell et al., 2021; D.K. Wyant et al., 2022; W. Burke et al., 2019). D. W. Kim et al., 2020 proposes a "Risk management-based security evaluation model for telemedicine systems" but this work has the following flaws.

a. Doesn't ensure end to end security
b. Doesn't ensure device security
c. Doesn't ensure network security
d. This work does not discuss the vulnerabilities in the application layer
e. This work does not discuss the vulnerabilities in the application layer
f. This work cannot withstand Reverse engineering attacks

Jofre M et al., (2021) proposes a "Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach" but this work has the following limitations

a. Doesn't ensure communication security
b. It does not propose a protocol
c. Doesn't ensure device security
d. This work does not discuss the vulnerabilities in the application layer
e. This work does not discuss the vulnerabilities in the application layer
f. This work cannot withstand Reverse engineering attacks

Mohd Javaid et al., (2023) identified and studied the applications of cybersecurity in healthcare but this work does not propose any novel work. L. Xiao et al., (2021) proposes an authentication scheme in Telecare Medical Information System (TMIS) using Physical Unclonable Function (PUF) and Elliptic Curve Cryptography (ECC) technology, but this work cannot withstand reverse engineering attacks. Patient's data is very valuable for the attackers, J. Müthing et al., (2017) highlights issues in transport layer in the mobile Healthcare frameworks, then proposes a platform for testing and framework in order to overcome these attacks. J. Müthing et al., (2019) highlights server side security issues and weaknesses in the mobile health applications and then compares with the other applications. B.M. Silva et al., (2013) proposes a data encryption solution for mobile health applications (DE4MHA).

a) Cannot adhere with HIPAA standards.
b) Fails to ensure application security
c) Fails to ensure Communication security

In order to overcome these limitations, we propose a Secure and Resilient Framework for Internet of Medical Things (IoMT) with an Effective Cybersecurity Risk Management. Our proposed framework ensures device Level security using UICC (Universal Integrated Circuit Card), TPM (Trusted Platform Module), Network level security is ensured using SSL/TLS protocol thereby ensuring communication security and Storage and Processing Level security is ensured using homomorphic encryption at the server side. This article's organization is as follows: In Section II we propose a Secure IoMT framework. Section III presents results and discussion and Section IV concludes the paper.

2. Proposed Secure IoMT Framework

2.1. Risk Computation in Internet of Medical Things (IoMT)

We propose a novel approach to compute risk for Internet of Medical Things (IoMT). The risk of any device 'd' is calculated as **r(d)=w(d) x s(d)**, where w(d) is the potential risk impact due to the attacks and vulnerabilities in the mobile application, hardware of the mobile device and server. 's' represents the likelihood of the risk.

S.No	Risk Impact Parameter (RIP)	RIP types	Weights (W)
1	Type of Network (NW)	Insecure Network	10
		Network with minimum Security	5
		Completely secured Network	2
2	Protocol Prone to Attacks (PRT)	Prone to more attacks	10
		Prone to fewer attacks	5
		Not prone to attacks	2
3	Use of Trusted Platform Module (TPM) and Secure Element (SE)	Completely unsecured device	10
		Partially secured device	5
		Totally secured device	2
4	Application Security (AS)	Completely insecure	10
		Partially secure	5
		Completely secure	2
5	Reverse Engineering Attacks (REA)	Completely insecure	10
		Partially secure	5
		Completely secure	2
6	Communication Security (CS)	Completely insecure	10
		Partially secure	5
		Completely secure	2
7	Defense In Depth Approach (DiDA)	Completely insecure	10
		Partially secure	5
		Completely secure	2

Table. 1: Risk Impact Parameters with their weights

S.No	Risk Impact Parameter (RIP)	RIP types	Weights (W)	's' likelihood of the risk	Risk of any device 'd' r(d)=w(d) x s(d)
1	Type of Network (NW)	Insecure Network	10	0.8	8
		Network with minimum Security	5	0.8	4
		Completely secured Network	2	0.8	1.6
2	Protocol Prone to Attacks (PRT)	Prone to more attacks	10	0.8	8
		Prone to fewer attacks	5	0.8	4
		Not prone to attacks	2	0.8	1.6
3	Use of Trusted Platform Module (TPM) and Secure Element (SE)	Completely unsecured device	10	1	10
		Partially secured device	5	1	5
		Totally secured device	2	1	2
4	Application Security (AS)	Completely insecure	10	1	10
		Partially secure	5	1	5
		Completely secure	2	1	2
5	Reverse Engineering Attacks (REA)	Completely insecure	10	1	10
		Partially secure	5	1	5
		Completely secure	2	1	2
6	Communication Security (CS)	Completely insecure	10	1	10
		Partially secure	5	1	5
		Completely secure	2	1	2
7	Defense In Depth Approach (DiDA)	Completely insecure	10	1	10
		Partially secure	5	1	5
		Completely secure	2	1	2

Table 2. Risk Calculation of the Device

Table 1 shows the Risk Impact Parameters (RIP) with their weights and RIP types. We have calculated the Risk of a Device in Table 2.

a) **Type of the network:** An insecure network ensures no security and privacy and the risk impact would be the maximum. These networks compromise the confidentiality, integrity and availability properties.

b) **Protocol Prone to Attacks (PRT)**: Existing Internet of Medical Things (IoMT) solutions are vulnerable to attacks on the device level, network level, communication level and application level.

c) **Use of Trusted Platform Module (TPM) and Secure Element (SE):** It is very difficult to compromise the integrity of Trusted Platform Module (TPM), so applications installed in the TPM and Secure Element (SE) are free from vulnerabilities, so applications installed on the SE and TPM cannot be compromised.

d) **Application Security (AS):** Internet of Medical Things (IoMT) frameworks needs to ensure application security by adopting cryptographic algorithms.

e) **Reverse Engineering Attacks (REA):** Mobile Healthcare Applications (MHA) in the Internet of Medical Things (IoMT) frameworks are prone to reverse engineering attacks

f) **Communication Security (CS):** Internet of Medical Things (IoMT) frameworks needs to ensure communication security, it is ensured using SSL/TLS protocols.

g) **Defense in Depth Approach (DiDA): S**ecurity should be a part of the Internet of Medical Things (IoMT) framework from the initial phase. Security should be implemented at all the levels such as communication security, application security and device security.

2.2. Risk Calculation based upon the Threat Events in Internet of Medical Things (IoMT)

This section calculates the Risks in the Internet of Medical Things (IoMT) realm based upon the Threat Events. Table 3 shows the Risk Calculation based upon the Threat Events in IoMT. Following are the threat events which are very critical in IoMT environment.

a) Reverse Engineering Attacks: Mobile Healthcare Applications (MHA) in the Internet of Medical Things (IoMT) frameworks are prone to reverse engineering attacks. These attacks are anticipated attacks. We propose to overcome these by using obfuscation techniques.

b) **Communication Security Attacks:** The risk associated with communication security are more in Internet of Medical Things (IoMT) frameworks, so in order to ensure communication security SSL/TLS protocols are used.

c) **Application Security Attacks:** The risk associated with application security are more in Internet of Medical Things (IoMT) frameworks. In order to ensure application security cryptographically algorithms should be used for encryption and digital signatures.

d) Multi-Protocol Attacks: A multi-protocol attack is an attack against an authentication protocol that uses messages generated from a separate protocol (not just another run of the same protocol) to spoof one of the participants into successfully completing the protocol. The risk associated with multi-protocol attacks are more in Internet of Medical Things (IoMT) frameworks. In order to ensure security against these attacks we need to use cryptographically algorithms which are used for encryption and digital signatures.

e) **Credentials are not generated and stored in Secure Element and Trusted Platform Module:** The risks associated with the credentials generated and **s**tored in the Secure Element and Trusted Platform Module are more in Internet of Medical Things (IoMT) frameworks as it is very difficult to compromise the integrity of Trusted Platform Module (TPM), so applications installed in the TPM and Secure Element (SE) are free from vulnerabilities, so applications installed on the SE and TPM cannot be compromised.

3. Results and Discussion

PILAR Risk Management Tool

Risk analysis identifies inherent risks in information and communication technologies. Risk damages the information and communication services of the organization. Risk analysis has a scientific approach:

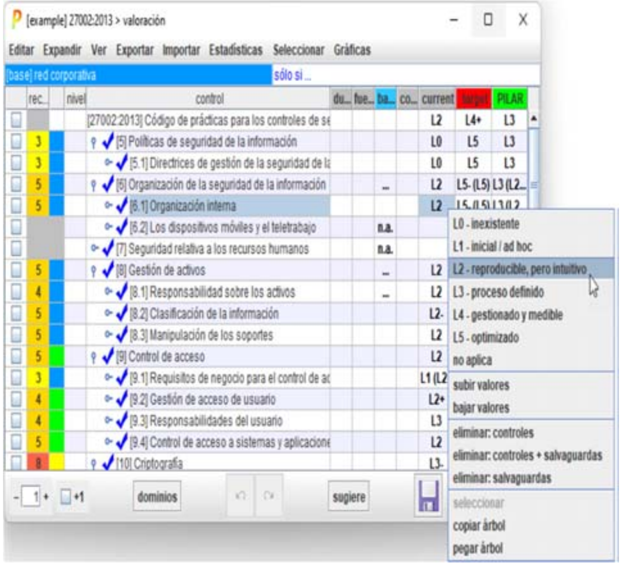
a. identifies the assets to protect

b. identify the important entities in the information and communication technologies that support the assets, where attacks may cause harm

c. Provide secure solutions in order to withstand against attacks

d. Evaluate the indicators with facts and figures in order to help decision makers to arrive for a good decision.

In a qualitative analysis, the probability is measured using a corresponding scale using low, moderate and high terms. This method of risk assessment involves a subjective measure of estimation and is easy to perform. However, it is less accurate than the quantitative risk assessment. PILAR Risk Management Tool is a tool used to perform qualitative and quantitative risk analysis. In order to implement risk analysis, we have used PILAR Risk Management Tool. PILAR Risk Management Tool analyzes both qualitative and quantitative risk analysis for longer periods thereby providing incremental analysis. Following are the results using PILAR tool.



	rec.		nivel	control	du...	fue...	ba...	co...	current	target	PILAR
□				[27002:2013] Código de prácticas para los controles de se					L2	L4+	L3
□	3	🟦		[5] Políticas de seguridad de la información					L0	L5	L3
□	3	🟦		[5.1] Directrices de gestión de la seguridad de la					L0	L5	L3
□	5	🟦		[6] Organización de la seguridad de la información			–		L2	L5- (L5)	L3 (L2...
□	5	🟦		[6.1] Organización interna					L2	L5 (L5)	L3 (L2
□				[6.2] Los dispositivos móviles y el teletrabajo			n.a.				
□				[7] Seguridad relativa a los recursos humanos			n.a.				
□	5	🟦		[8] Gestión de activos			–		L2		
□	4	🟦		[8.1] Responsabilidad sobre los activos			–		L2		
□	5	🟦		[8.2] Clasificación de la información					L2-		
□	5	🟦		[8.3] Manipulación de los soportes					L2		
□	5	🟩		[9] Control de acceso					L2		
□	3	🟦		[9.1] Requisitos de negocio para el control de ac					L1 (L2		
□	4	🟩		[9.2] Gestión de acceso de usuario					L2+		
□	4	🟩		[9.3] Responsabilidades del usuario					L3		
□	5	🟩		[9.4] Control de acceso a sistemas y aplicacione					L2		
□	8	🟨		[10] Criptografía					L3-		

Fig. 1: Results using PILAR TOOL

4. Conclusion

We have proposed a secure and resilient framework for IoMT by computing the risk using Risk Impact Parameters (RIP) and based upon the Threat Events in the Internet of Medical Things (IoMT). UICC (Universal Integrated Circuit Card) and TPM (Trusted Platform Module) play very important role in ensuring security in IoMT. Internet of Medical Things (IoMT) played very crucial role during COVID-19 pandemic by providing healthcare services anywhere and at any time. In order to implement risk analysis, we have used PILAR Risk Management Tool. PILAR Risk Management Tool analyzes both qualitative and quantitative risk analysis for longer periods thereby providing incremental analysis.

References

[1] D.N. Burrell, A.S. Aridi, Q. McLester, A. Shufutinsky, C. Nobles, M. Dawson, S.R. Muller (2021). Exploring system thinking leadership approaches to the healthcare cybersecurity environment, Int. J. Extreme Autom. Connect. Healthc. (IJEACH) 3 (2) (2021) 20–32 .

[2] D.K. Wyant, P. Bingi, J.R. Knight, A. Rangarajan (2022). Deter framework: a novel paradigm for addressing cybersecurity concerns in mobile healthcare, Res. Anthol. Secur. Med. Syst. Rec. (2022) 381–407 .

[3] W. Burke, T. Oseni, A. Jolfaei, I. Gondal (2019). Cybersecurity indexes for eHealth, in: Proceedings of the Australasian Computer Science Week Multiconference, 2019, pp. 1–8 .

[4] D. W. Kim, J.Y. Choi and K.H. Han (2020). “Risk management-based security evaluation model for telemedicine systems,” *BMC Medical Informatics Decision Making*, vol.20, no.1, pp.1-14,2020. [doi: 10.1186/s12911-020-01145-7] [Medline: 32522216]

[5] Jofre M, Navarro-Llobet D, Agulló R, Puig J, Gonzalez-Granadillo G, Mora Zamorano J, Romeu R. (2021). Cybersecurity and Privacy Risk Assessment of

Point-of-Care Systems in Healthcare—A Use Case Approach. *Applied Sciences*. 2021; 11(15):6699. https://doi.org/10.3390/app11156699

[6] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Rajiv Suman (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends, Cyber Security and Applications, Volume 1, 2023, 100016,ISSN 2772-9184, https://doi.org/10.1016/j.csa.2023.100016.

[7] L. Xiao, S. Xie, D. Han, W. Liang, J. Guo *et al.,* (2021). "A lightweight authentication scheme for telecare medical information system," *Connection Science,* vol.33, no.3, pp.769-785, 2021 [doi: 10.1080/09540091.2021.1889976]

[8] J. Müthing, T. Jäschke and C. M. Friedrich (2017). "Client-Focused Security Assessment of mHealth Apps and Recommended Practices to Prevent or Mitigate Transport Security Issues," *JMIR Mhealth Uhealth,* vol.5, no.10: e147, 2017 [doi: 10.2196/mhealth.7791]

[9] J. Müthing, R. Brüngel and C.M. Friedrich (2019). "Server-Focused Security Assessment of Mobile Health Apps for Popular Mobile Platforms," *Journal Medical Internet Research,* vol.21, no.1*:* e9818, 2019 [doi: 10.2196/jmir.9818]

[10] B.M. Silva, J.JPC. Rodrigues, F. Canelo, I.C. Lopes and L. Zhou (2013). "A Data Encryption Solution for Mobile Health Apps in Cooperation Environments," *Journal Medical Internet Research,* vol.15, no.4*:* e66, 2013 [doi: 10.2196/jmir.2498]

[11] PILAR Risk Management Tool https://www.pilar-tools.com/en/

Latifah Khalid Alabdulwahhab is currently pursuing her Master's in Cybersecurity and Digital Forensics at the Department of Information Technology, College of Computer and Information Sciences Majmaah University, Al-Majmaah, 11952, Saudi Arabia. She can be contacted at Lia910x@gmail.com and 431204720@s.mu.edu.sa

Dr. Shaik Shakeel Ahamad is currently working as an Associate Professor in CCIS, Majmaah University, Kingdom of Saudi Arabia. He holds a PhD in Computer Science from the University of Hyderabad (a Central University which ranks second in India) and IDRBT (Institute For Development and Research in Banking Technology), Hyderabad, India in the realm of secure mobile payments protocols and formal verification. He has published more than 25 research papers in reputed International journals / Proceedings indexed by ISI, Scopus, ACM Digital Library, DBLP and IEEE Digital Library. He is serving as a Review Committee Member in many ISI indexed journals. He is CEI (Certified EC Council Instructor), ECSA (EC Council Certified Security Analyst), CHFI (Computer Hacking Forensic Investigator), Certified Threat Intelligence Analyst (CTIA) and Certified Application Security Engineer (CASE) – Java. His research interests include cloud-based mobile commerce, secure mobile healthcare frameworks, Block chain technology, Application Security and Smart Grids. He is a member of IEEE, Association for Computing Machinery (ACM), ISACA and OWASP (Open Web Application Security Project). He can be reached at ahamadss786@gmail.com & s.ahamad@mu.edu.sa