LE STUDIUM
Loire Valley
Institute for Advanced Studies

LE STUDIUM Multidisciplinary Journal
ISSN 2669-7807

www.lestudium-ias.com

FELLOWSHIP FINAL REPORT

A Security Architecture for the Internet of Medical Things

Marko Hölbl[1,3], Patrice Clemente[2]

[1] University of Maribor, Maribor, Slovenia

[2] LIFO, INSA Centre Val de Loire, Bourges, France

[3] LE STUDIUM Institute for Advanced Studies, 45000 Orléans, France

REPORT INFO

Fellow: ***Marko Hölbl***
From the University of Maribor, Faculty of Electrical Engineering and Computer Science, Maribor, Slovenia
Host laboratory in region Centre-Val de Loire: Systems Distribution and Security (SDS), Orléans Computer Science Laboratory (LIFO), INSA Centre Val de Loire
Host scientist: ***Patrice Clemente***
Period of residence in region Centre-Val de Loire: May 2023 – August 2023

ABSTRACT

This paper presents a security architecture for the Internet of Medical Things (IoMT), striving to protect sensitive data stored, processed, and transferred in such a system. It is based on a 5-layer architecture for IoMT systems and defines security mechanisms and techniques that can be employed on the different layers in order to protect medical data in its whole lifecycle adequately. Additionally, we also discuss the most common security requirements and attacks from literature which served as the basis for the security architecture. The former can be implemented on various heterogenous IoMT devices and environments.

Keywords :
Internet of medical things; authentication; access control; data security; privacy; architecture.

1- Introduction

The Internet of Medical Things (IoMT) connects medical sensors, equipment, apps, wearable medical equipment, and smart sensors and thus provides the possibility of real-time health monitoring [1]. In this context, distributed information architecture solutions connect medical applications to data sources with decreased latency and improved portability, quality of service, engagement, and characterization [2]. IoMT-based healthcare solutions use these capabilities to make medical treatments more efficient, fast, and accessible. Empowering patients helps doctors intervene by making them aware of and in control of their health [1]. It will particularly benefit distant communities, underdeveloped nations, and disaster-stricken areas where healthcare specialists are few [3].

However, scalable, reliable, and resilient designs are needed for IoMT-based healthcare monitoring systems [4]. Therefore, the security of IoMT and healthcare systems is vital since such systems handle healthcare data. Hence protection measures should be taken during collection, transmission, and storage in such environments. In 2020, CyberMDX found that over 50% of IoMT devices are vulnerable [5].

The security and privacy aspects of IoMT are unique since they can affect patients' lives, and the data handled in these environments is particularly sensitive. Thus, IoMT systems need security to be widely adopted, but power consumption and different constraints of IoMT-based systems limit and burden the use of conventional security mechanisms and approaches.

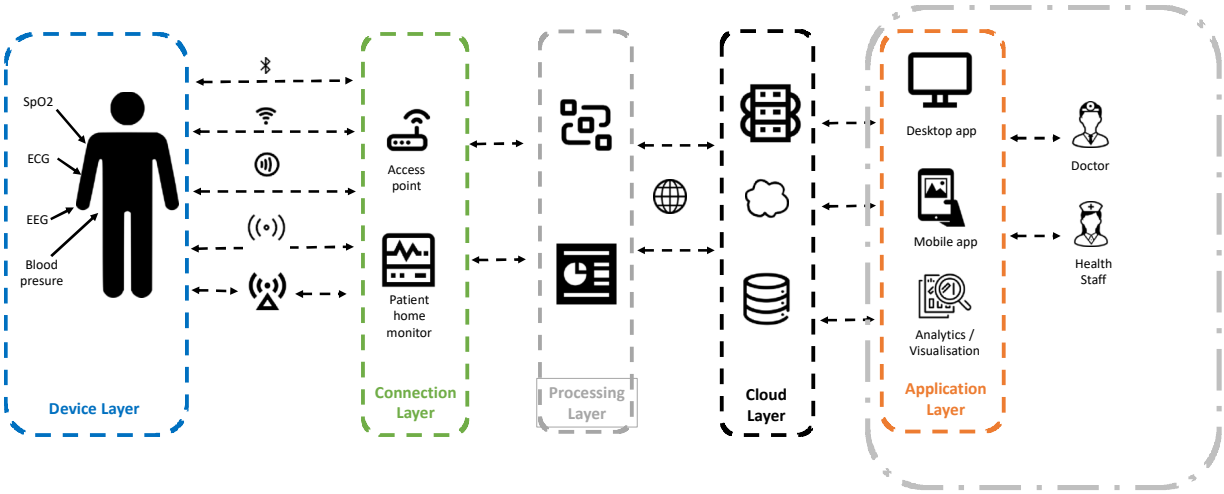

Figure 1: IoMT Architecture

1.1- Architecture of IoMT

IoMT is a sophisticated and interconnected system that facilitates communication and data exchange between medical devices, sensors, and healthcare systems. IoMT architecture supports the integration and administration of a vast network of devices, such as wearable health monitors, remote monitoring systems, smart medical implants, and healthcare infrastructure. IoMT architecture is comprised of multiple layers to facilitate the transmission, processing, and use of medical data. In healthcare settings, IoMT architecture enables real-time monitoring, secure data transmission, interoperability, and intelligent decision-making by leveraging cloud computing, periphery computing, and advanced networking technologies. This interconnected framework not only improves patient care, diagnosis, and treatment but also paves the way for personalized medicine, remote healthcare, and enhanced healthcare administration as a whole.

In this paper, the IoMT architecture is defined using the five strata depicted in Figure 1.

2- Security of IoMET

In the context of IoMT security, we need to be aware that such systems comprise interconnected sensors and devices linked to cloud ecosystems via the Internet [6]. Cloud services receive data acquired from these devices/sensors to cleanse and further process these data to gain deeper comprehension. Additionally, Io(M)T utilizes numerous wireless technologies, including Near Field Communications (NFC), Bluetooth (and Bluetooth Low Energy, or BLE), or LTE/5G/6G [6]. These technologies are interconnected with numerous devices, including smartphones, monitoring equipment, sensors, smart wearables, and other medical devices [6].

All these aspects need to be taken into consideration when developing security mechanisms, such as a security architecture.

2.1- Security Requirements of IoMT

From collection to transmission and storage, IoMT systems must protect patient data [7].

The sensor layer of an IoMT system collects patient data. Sensor hardware manipulation and data tampering are possible now. Patients could die if the sensor's hardware or software is hacked. Thus, protecting data from these risks is crucial to system maintenance.

All device communications, including between IoMT sensors in the sensor layer and the access point (AP) in the intermediate layer, need to be protected. Attacks here can change or interrupt sensor data transmission. Thus, preventing such attacks is crucial.

The connection, processing, and cloud layers collect and store patient data. Because most of the data in this layer are "asleep" most of the

time, they are more vulnerable to unauthorized access than data on any other layer.

Due to patient data's sensitivity and safety, IoMT systems must include security mechanisms at all layers. These include confidentiality, integrity, non-repudiation, authentication, authorization, anonymity, forward/backward secrecy, key exchange, key-escrow resilience, (session) key agreement [8].

2.2- Attacks on IoMT

Because effective decision-making necessitates sophisticated patient monitoring and enormous patient data, the use of IoMTs will increase. It is anticipated that the risks to security will continue to grow. Consequently, protection mechanisms and measures need to be comprehensive.

Physical attacks target IoMT sensors and keys to steal patient data or security keys. The attacker must physically access a specific IoMT system component. These aspects include the following attacks: loss of physical security tokens, impersonation/masquerading, tampering, or side-channel attacks [10], [11].

An adversary can compromise the integrity of information by intercepting both data in transit and data at rest. They employ the following techniques to conduct information-based attacks: interception, modification, fabrication, replay attack, and interruption attack [10], [11].

Attacks on hosts are carried out by exploiting the host's characteristics, including user compromise, hardware compromise, and software compromise [10], [11].

Network-based attacks may target the communication between various IoMT system layers, such as Bluetooth or Internet connections. Typically, these attacks seek to steal or falsify patient data or block the relationships between the layers of IoMT systems. Attacks of such type include DoS/DDoS, sniffing, Man-in-the-Middle (MITM) attacks, replay attacks, parallel sessions, and brute force attacks [10], [11].

3- Proposed Security Architecture for IoMET

The proposed security architecture (cf. Figure 1) is based on the previous work [11], [12], [13]. We explain details about the architecture below for every layer foreseen in the architecture of the IoMT system.

Device Layer

Wearables, implants, and hospital equipment generate and gather data in the device layer. This layer's security measures include the following:

- Secure boot techniques restrict device software to manufacturer-approved software. To avoid malware, firmware updates should be digitally signed and authenticated.
- Verifying the device's identity before connecting to the network. Cryptographic keys, digital certificates, and shared secrets can authenticate devices. HSMs or TPMs can store cryptographic keys and execute secure operations in a tamper-proof environment [14].
- Data Encryption should be used. Symmetric encryption like AES-CCM or Adiantum [15] should safeguard data at rest and in transit from unauthorized access.
- Tamper-prone equipment needs physical security. Secure enclosures and tamper-evident seals prevent tampering. Tamper-resistant hardware can erase sensitive data if it detects physical tampering. Sensitive data and operations can use HRoT [16].

Connection Layer

Devices send data to this layer, and therefore, security mechanisms are tailored to this context and include:

- Security mechanisms for different communication protocols are essential. These include CoAP and MQTT [17] or, for wireless networks, mechanisms like WPA2 [18] or WPA3 [19].
- Before data transmission, the device and network should authenticate each other. As an example, mTLS can authenticate devices and networks [20].
- To prevent security breaches, network segments should isolate devices. VLANs or

firewalls can segment networks and isolate devices [21].

Processing (Edge) Layer

Edge computing reduces data transmission and exposure by processing data near its production. As with the previous layer, also this needs to be protected:

- Local data processing reduces data exposure during transmission. Edge computing platforms [22] process data near devices.
- Data anonymization can be protected by techniques like differential privacy [23]. However, one has then to address the utility problem of the data: as differential privacy tampers with the local data, to what extent the data is still useful for the immediate health care of the patient, in case of emergency for example.
- Locally monitor threats and suspicious activity. Local IDS can employ Snort [24].

Cloud Layer

The cloud Layer involves storing and processing additional data in the cloud, and the security measures include:

- Data access should be restricted using RBAC [25] and ABAC [26]. Additionally, encryption of all cloud data should be used.
- Many programs communicate via APIs. Secure these interfaces to prevent unauthorized access or abuse [27]. Use API keys or OAuth for API security [28].
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are applied to monitor and mitigate security breaches [29].
- Secure backup of data needs to be routine, and a disaster recovery plan must be in place.

Application Layer

The Application Layer is responsible for delivering data and insights to end consumers and can be protected by:

- Secure application development - secure coding practices should be used to minimize attacker vulnerabilities in applications. Input validation, error handling, and secure APIs prevent injection attacks and information leaks.
- Regular patching and updates. Patching and updating apps regularly mitigate known vulnerabilities. A vulnerability management approach should comprise vulnerability scanning, risk assessment, patch testing, and deployment.
- User authentication and authorization. Strong authentication controls application access. Biometric, multi-factor or behavioral authentication may be used. After authentication, an authorization process should restrict users to authorized services and data.
- Multi-factor authentication should be used to authenticate users [30].
- Access control techniques should restrict users to data and functions relevant to their responsibilities [31].
- Applications should encrypt sensitive data at rest and in transit. Use strong encryption and key management [32].
- Privacy-by-Design - consider privacy throughout program development and operation [33]. Data minimization, where only essential data is collected and used, and anonymization or pseudonymization, where identifying information is removed or altered to prevent identification, may be employed.

Audit and Logging - applications should log user activities, system events, and faults 0. These logs can help detect and investigate security breaches and provide proof.]

4- Conclusion

Due to the rising demand for IoMT sensors to reduce healthcare costs and enhance patient care, securing these devices has become essential. Nevertheless, IoMT sensors typically have limited resources and securing already implanted sensors requires external devices. In this paper, we proposed an architecture that employs a combination of these techniques to satisfy all security requirements since no single approach can mitigate the preponderance of attacks and meet the security requirements of these systems. It covers all data and device

security phases, commencing with data collection and extending to data storage and sharing.

5- Perspectives of future collaborations with the host laboratory

The collaboration with the host laboratory and scientists is ongoing. A paper is currently in preparation with the results achieved during the visit. Additionally, the collaboration will be expanded in the aspect of internship exchanges, Erasmus mobilities, and continuation of research in the field of security and privacy of the Internet of medical things.

6- Articles published in the framework of the fellowship

The outcome of this work will result in a journal paper which is currently in a draft version and will be finalized and submitted for publication shortly.

7- Acknowledgements

This work was supported by the "Le Studium ATHENA Visiting Researcher Program".

8- References

[1] J. N. S. Rubí and P. R. L. Gondim, "IoMT Platform for Pervasive Healthcare Data Aggregation, Processing, and Sharing Based on OneM2M and OpenEHR," Sensors, vol. 19, no. 19, 2019, doi: 10.3390/s19194283.

[2] N. S. Abul-Husn and E. E. Kenny, "Personalized Medicine and the Power of Electronic Health Records," Cell, vol. 177, no. 1, pp. 58–69, 2019, doi: https://doi.org/10.1016/j.cell.2019.02.039.

[3] M. A. Khan and F. Algarni, "A Healthcare Monitoring System for the Diagnosis of Heart Disease in the IoMT Cloud Environment Using MSSO-ANFIS," IEEE Access, vol. 8, pp. 122259–122269, Jun. 2020, doi: 10.1109/ACCESS.2020.3006424.

[4] G. Villarrubia, J. Bajo, J. F. De Paz, and J. M. Corchado, "Monitoring and Detection Platform to Prevent Anomalous Situations in Home Care," Sensors, vol. 14, no. 6, pp. 9900–9921, 2014, doi: 10.3390/s140609900.

[5] N. Y. N. U. CyberMDX, "2020 Vision: A Review of Major IT & Cyber Security Issues Affecting Healthcare," 2020. Accessed: Jun. 29, 2023. [Online]. Available: https://www.healthcareinfosecurity.com/whitepapers/2020-vision-review-major-cybersecurity-issues-affecting-healthcare-w-6017

[6] 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, Jul. 2022, doi: 10.1080/02564602.2021.1927863.

[7] M. Cäsar, T. Pawelke, J. Steffan, and G. Terhorst, "A survey on Bluetooth Low Energy security and privacy," Computer Networks, vol. 205, p. 108712, 2022, doi: https://doi.org/10.1016/j.comnet.2021.108712.

[8] N. Garg, M. Wazid, J. Singh, D. P. Singh, and A. K. Das, "Security in IoMT-driven smart healthcare: A comprehensive review and open challenges," SECURITY AND PRIVACY, vol. 5, no. 5, p. e235, 2022, doi: https://doi.org/10.1002/spy2.235.

[9] R. Yugha and S. Chithra, "A survey on technologies and security protocols: Reference for future generation IoT," Journal of Network and Computer Applications, vol. 169, p. 102763, 2020.

[10] M. Papaioannou et al., "A survey on security threats and countermeasures in internet of medical things (IoMT)," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 6, p. e4049, 2022.

[11] M. Papaioannou et al., "A survey on security threats and countermeasures in internet of medical things (IoMT)," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 6, p. e4049, 2022.

[12] P. S. R. M. S. R. Vankamamidi S. Naresh Suryateja S. Pericherla, "Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions," Computer Systems Science and Engineering, vol. 35,

no. 6, pp. 411–421, 2020, doi: 10.32604/csse.2020.35.411.
[13] D. Nkomo and R. Brown, “Hybrid Cyber Security Framework for the Internet of Medical Things,” in Blockchain and Clinical Trial: Securing Patient Data, H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, and H. Al-Khateeb, Eds., Cham: Springer International Publishing, 2019, pp. 211–229. doi: 10.1007/978-3-030-11289-9_9.
[14] A. Al-Omary, A. Othman, H. M. AlSabbagh, and H. Al-Rizzo, “Survey of hardware-based security support for IoT/CPS systems,” KnE Engineering, pp. 52–70, 2018.
[15] P. Crowley and E. Biggers, “Adiantum: length-preserving encryption for entry-level processors.” 2018. [Online]. Available: https://eprint.iacr.org/2018/720
[16] J. Frazelle, “Securing the Boot Process: The Hardware Root of Trust,” Queue, vol. 17, no. 6, pp. 5–21, Feb. 2020, doi: 10.1145/3380774.3382016.
[17] V. Seoane, C. Garcia-Rubio, F. Almenares, and C. Campo, “Performance evaluation of CoAP and MQTT with security support for IoT environments,” Computer Networks, vol. 197, p. 108338, 2021, doi: https://doi.org/10.1016/j.comnet.2021.108338.
[18] I. and A. R. and A. A. Khasawneh Mahmoud and Kajman, “A Survey on Wi-Fi Protocols: WPA and WPA2,” in Recent Trends in Computer Networks and Distributed Systems Security, S. M. and K. R. and S. L. Martínez Pérez Gregorio and Thampi, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 496–511.
[19] K. Lounis and M. Zulkernine, “WPA3 Connection Deprivation Attacks,” in Risks and Security of Internet and Systems: 14th International Conference, CRiSIS 2019, Hammamet, Tunisia, October 29–31, 2019, Proceedings, Berlin, Heidelberg: Springer-Verlag, 2019, pp. 164–176. doi: 10.1007/978-3-030-41568-6_11.
[20] B. Campbell, J. Bradley, N. Sakimura, and T. Lodderstedt, “RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens.” 2020.
[21] A. F. Gentile, P. Fazio, and G. Miceli, “A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios,” in Telecom, MDPI, 2021, pp. 430–445.
[22] M. Hartmann, U. S. Hashmi, and A. Imran, “Edge computing in smart health care systems: Review, challenges, and research directions,” Transactions on Emerging Telecommunications Technologies, vol. 33, no. 3, p. e3710, 2022.
[23] A. Majeed and S. Lee, “Anonymization techniques for privacy preserving data publishing: A comprehensive survey,” IEEE access, vol. 9, pp. 8512–8545, 2020.
[24] A. Waleed, A. F. Jamali, and A. Masood, “Which open-source IDS? Snort, Suricata or Zeek,” Computer Networks, vol. 213, p. 109116, 2022.
[25] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, “Proposed NIST Standard for Role-Based Access Control,” ACM Trans. Inf. Syst. Secur., vol. 4, no. 3, pp. 224–274, Aug. 2001, doi: 10.1145/501978.501980.
[26] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, “Attribute-Based Access Control,” Computer (Long Beach Calif), vol. 48, no. 2, pp. 85–88, Feb. 2015, doi: 10.1109/MC.2015.33.
[27] R. Badhwar, “Intro to API Security-Issues and Some Solutions!,” in The CISO’s Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms, Springer, 2021, pp. 239–244.
[28] Y. Acar, C. Stransky, D. Wermke, C. Weir, M. L. Mazurek, and S. Fahl, “Developers Need Support, Too: A Survey of Security Advice for Software Developers,” in 2017 IEEE Cybersecurity Development (SecDev), Sep. 2017, pp. 22–26. doi: 10.1109/SecDev.2017.17.
[29] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, “A survey on intrusion detection and prevention systems in digital substations,” Computer Networks, vol. 184, p. 107679, 2021.
[30] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-factor authentication:

A survey," Cryptography, vol. 2, no. 1, p. 1, 2018.
[31] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," IEEE Internet Things J, vol. 7, no. 6, pp. 4682–4696, 2020.
[32] A. Bouriche and S. Bouriche, "A systematic review on security vulnerabilities to preveny types of attacks in iomt," International Journal of Computations, Information and Manufacturing (IJCIM), vol. 2, no. 2, 2022.
[33] R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and privacy management in Internet of Medical Things (IoMT): A synthesis," Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 640–661, 2022.

Y. S. Huilgol, J. Adler-Milstein, S. L. Ivey, and J. C. Hong, "Opportunities to use electronic health record audit logs to improve cancer care," Cancer Med, vol. 11, no. 17, pp. 3296–3303, 2022.