Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Cybersecurity Approach in Internet of Healthcare Things (IoHTs)

Mohammad Furqan Ali

COPELABS – Lusófona University, Lisbon, Portugal
Email: mohammadfurqanali@gmail.com

Abstract

A huge demand of internet connecting devices in medical field is crucial for patient assistance. The current trends in healthcare industries, the internet of things (IoTs) play an ample role for nodes connectivity in wireless domain. The main purpose of the integrated internet of healthcare things (IoHTs) as well as internet of medical things (IoMTs) is the real-time observation of patients and provide healthcare comfort zone for individuals. Emergence of novel treatment methodology and medical tools encourage delivering services for IoHT domain. Due to lack of publicly useful database, that reflects cyberattacks on IoHT, expendability privacy concern. Therefore, this study highlights the secure services to the current challenges and overviewed the solution of secured services targeting on IoHT attacks.

Keywords: Internet of Healthcare Things, Cyber Attack, IoT

Citation: M. F. Ali, “IoHTs: Cybersecurity Approach in Internet of Healthcare Things”, ARIS2-Journal, vol. 3, no. 2, pp. 26–33, Dec. 2023.

DOI: https://doi.org/10.56394/aris2.v3i2.32

* Corresponding author. Email address: mohammadfurqanali@gmail.com

1. Introduction (use bold for main headings like this one. do not use italic)

The healthcare industry is rapidly growing up in comparison of last decades. It proliferates due to the involvement of internet of things (IoTs) possibly in every aspect. The internet-connected devices are quite useful to support an assisting life of patient [1]. Additionally, the IoT plays a significant role and their properties in the life of humanitarian aid with the incorporation of IoT in medical care related to internet of healthcare things (IoHTs). The internet of health care types of equipment which are more useful in providing real health-related data and directly linked to the corresponding doctor or specialist, often demonstrate the specific need to cure the patient. Furthermore, the IoHTs offer a solution to discuss the factors and the prevention of disease. It can be assumed that it would be useful in supporting and improving life in the future with high accuracy along with well-equipped consumer products and differentiated services [2]. A potential future outcome is that the corporations will contribute to increase their offerings and extend their value proposition to other health care concerns. An involvement internet of healthcare things (IoHT) and selling or sharing very sensitive data raised the cybersecurity issue of misusing patients' privacy. The outcomes of IoHT emphasize an advancement of healthcare digitalization. The sensors support data collection, analysis, and enhance the medical services. Currently, the IoHT industries have a big impact on various medical applications [3]. It is noteworthy that the reliability and capability of medical devices with patient's body is quite significant nevertheless, the lack of security. Security vulnerabilities are severe and widespread in both wireless and wired medical devices [4]. It must take into consideration of applying security to protect the threat from online hackers. Therefore, the necessity to secure communication in medical devices does significance for smooth functioning and improving efficiency. Due to this concern this study is overviewed the possibilities of securing medical device communication.

1.1. The Five Layers of Concept of Cybersecurity

This study presents the privacy and security events and detection in internet of medical devices. Additionally, an intelligent interactive safety, security risks, and ambient intelligence approaches are overviewed. Concerning the security and privacy for IoHT framework, the primary contribution of reviewing five layers, and this study provides an extensive review on privacy and security as follows.

- **The Perception Layer**: - This layer is associated with the patients, medical tools for data collection, and hospital infrastructure. The perception layer prevents from unwanted common attacks such as malware, phishing, eavesdropping, and log-forgery.
- **Mist Layer**: - The mist layer receives real-data from perception layer for further optimization. This layer corresponds between the perception and fog-layer that contain micro storage and embedded systems. It is noteworthy that in this layer the common attacks are included as eavesdropping, wormhole, collision, fragmentation, side-channel, and masquerade.
- **Fog Layer**: - Minimizing the latency of processing and storing data in secured cloud computing the fog-layer introduces as gateway to improve the system performance. It generates real-time alerts that can be capable to control the response. The denial-of-services (DoS), scrambling, sniffing, and data tampering affect to this layer.
- **Cloud Layer**: - The processed healthcare data from fog-layer stored in the cloud that performs various

data analytics. Additionally, artificial intelligence (AI), machine learning (ML), and reasoning-based algorithms utilize for data analytics in the cloud computing. In this layer the interference, stealing password, eavesdropping, and data mining are included.

- **Application Layer**: - It is the topmost layer of confirming the secure communication between communication protocols at user end. The communication layer easily faces attacks due to lack of highly skilled engineers. The most significant vulnerability of data corruption, malware, phishing, and further attacks.

1.2. Implementation of 5G security and privacy in IoHT

The main purpose of this study is overviewed the security towards 5GB-based secure transmission of health information and sharing with multiple data servers. Also, the use of cryptosystems to execute statistical analysis of patient information without sacrificing patient confidentiality disclosed by the patient database administrator. Therefore, the following approaches are widely used for the security and privacy concerns in IoHT depicted as follows [5];

- Access Control: The access control can be operated by using the computer unit or a specific device such as a USB-security key.
- Secure Communication: The communication encryption can be deployed at the hardware level to secure the input and output ports for authentication of accessing applications and functions.
- Privacy Protection and data encryption: The limitation of the data for authorization of users are the most common measures to ensure about the privacy. Therefore, the privacy is highly concerning in wireless communication domain while connecting multiple nodes.

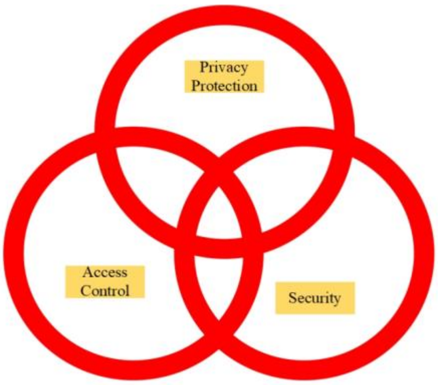

Fig. 1: A scenario of measures for robust cloud computing [5]

1.3. Massive Machine Type Communication (mMTC) in IoHT

The use of m-Health technology enables healthcare professionals to enhance their capabilities, facilitates proactive management of care, and encourages active engagement of patients. This is achieved via the utilization of various applications, such as remote patient monitoring, smart healthcare infrastructure, telemedicine, and health and wellness monitoring [6]. In order to fully harness the capabilities of mMTC in IoHT, it is imperative to address challenges pertaining to scalability, network congestion, power consumption, and data security. The healthcare industry has the potential to adopt a connected and patient-centric strategy by adopting advances developed by mMTC. These factors are expected to result in improved patient outcomes, increased healthcare accessibility, and significant advancements in healthcare service delivery [7].

Ensuring the security and privacy of sensitive healthcare data sent via wireless communication in IoHT necessitates a strong focus on both aspects [8]. In order to safeguard patient information, mitigate unauthorized access, and ensure adherence to regulatory obligations, it is essential to implement rigorous security protocols like as encryption, authentication, and access control.

1.4. Network Slicing and Security in IoHT

In the context of IoHT, the issues of network slicing and security assume paramount importance, as they play a critical role in ensuring the efficient and secure operation of interconnected devices and services [9]. In the context of IoHT networks, the concept of network slicing enables efficient resource allocation, provision of distinct services, scalability, and flexibility. The implementation of robust security measures is necessary in order to safeguard sensitive data, uphold patient privacy, and mitigate the risk of security breaches. The approaches to be considered should include device security, data privacy, access control, and interoperability, among other relevant factors. The successful use of IoT and IoHT networks in healthcare delivery relies upon the adoption and implementation of secure network slicing technologies and comprehensive security measures. This will enable the networks to maintain optimal levels of data integrity and secrecy while actualizing their full potential. This article examines the concept of network slicing and its utilization in the domains of IoHT. This also highlights the need of deploying robust security measures and addresses the challenges associated with ensuring the protection of interconnected networks [10].

2. Importance of Security in IoHT

The significance of security in the IoHT applications is important due to the sensitive nature of the data transmission and to mitigate the potential risks associated with compromised devices and networks. This importance stems from its role in safeguarding personal information, ensuring the integrity of healthcare data, mitigating unauthorized access, and minimizing potential cyber risks [11]. Moreover, the implementation of rigorous security measures is of utmost importance in order to instill trust, safeguard patient privacy, and uphold the confidentiality, availability, and reliability of healthcare services. Security measurements provides a secure environment for IoHT devices and networks via the implementation of robust authentication mechanisms, encryption protocols, access limitations, and proactive monitoring. This is essential to adhere to optimal security protocols, regularly update software, and undertake ongoing security evaluations to prevent the exploitation of emerging vulnerabilities and threats. Ensuring the safeguarding of healthcare systems and the privacy and well-being of patients necessitates prioritizing the security of IoHT applications [12]. Physical layer security (PLS) is a promising approach to improving the security and reliability of communication in the IoHT. PLS techniques exploit the physical properties of the wireless channel to protect data from eavesdropping and jamming. One of the key challenges in developing PLS techniques for IoHT is the resource-constrained nature of IoHT devices. IoHT devices often have limited processing power, memory, and energy resources. This makes it difficult to implement traditional PLS techniques, which can be computationally expensive. Another challenge is the unreliability of wireless channels. IoHT devices often communicate over wireless channels that are subject to noise and interference. This can make it difficult to reliably implement PLS techniques. Despite these challenges, there has been significant progress in developing PLS techniques for IoHT.

3. Security Challenges in IoHT

3.1 Device Vulnerabilities: IoHT devices often exhibit restricted resource availability and may exhibit deficiencies in robust security features. As a result, these entities are vulnerable to a diverse range of attacks, including data modification, unauthorized access, and the infiltration of malicious software. Safeguarding the comprehensive network of IoT and IIoT is imperative, necessitating the establishment of robust security measures to prevent these devices from serving as vulnerable access points for cyberattacks [13].

3.2 Data Privacy and Confidentiality: The IoHT Network are responsible for the reception and management of sensitive data, such as personal health information, medical records, and real-time patient monitoring data [14]. Therefore, preserving patient confidentiality and safeguarding the privacy of their data are of paramount importance in order to maintain patient trust and adhere to legal requirements. In order to safeguard patient data and mitigate the risk of unauthorized access or data breaches, it is essential to use strong encryption techniques, ensure secure data storage practices, and employ secure data transfer protocols.

3.3 Network Access Control: The Industrial Internet of Things networks must be secured through the implementation of strong access control measures in place because they reduce the possibility that unauthorized people or devices will get access. Strong authentication systems, secure access protocols, and network segmentation made possible by network slicing can all be used to reduce the dangers connected with unauthorized access and unauthorized data exposure [15]. Enforcing access control restrictions and periodically renewing access credentials are essential security protocols for protecting IIoT networks.

3.1 Interoperability and Standardization: The ecosystems of the IoT/IOHT include a wide range of devices, platforms, and protocols. The absence of interoperability and established security protocols across different components of the IoHT may give rise to possible security vulnerabilities [16]. Establishing industry-wide security standards and promoting interoperability are crucial in ensuring consistent and effective security measures across networks including the IoT and IoHT applications.

4. Security Measure for Network Slicing in IoHT

4.1 Isolation and Segmentation: When a network is partitioned, distinct services and applications are automatically separated and segregated from each other. Every component of the network operates independently, with its own dedicated resources, logical separation, and security protocols. As a result of this partition, any security breaches occurring inside one segment would not impact the other segments, hence ensuring the ongoing provision of critical healthcare services in a secure way.

4.2 Encryption and Authentication: Consequently, it has become imperative to include resilient encryption techniques and authentication protocols inside IoHT networks to safeguard data integrity and mitigate unauthorized intrusion. Secure communication channels include many techniques such as encryption mechanisms, secure key management, and mutual authentication between devices and network components [17]. These mechanisms serve to safeguard the transmission of information and ensure that only those with proper authorization are able to get access to the network.

4.3 Intrusion Detection and Prevention: In the context of IIoT networks, the implementation of intrusion detection and prevention systems (IDPS) may play a crucial role in the identification and mitigation of potential security vulnerabilities. Intrusion Detection and Prevention Systems (IDPS) are designed to oversee network traffic, do pattern analysis, and identify anomalies indicative of potential security breaches or hostile actions [18]. The mitigation of future damage to both the network and its associated devices may be achieved by the prompt detection of potential threats, followed by suitable and effective response measures.

4.4 Regular Updates and Patch Management: For the purpose of resolving security vulnerabilities, it's critical to handle frequent updates and patches for network infrastructure and IIoT devices. The prompt emphasizes the need of promptly installing recently announced security patches and firmware updates [19]. By doing so, organizations may effectively protect their networks against newly discovered vulnerabilities and maintain a resilient infrastructure in the face of emerging threats.

5. Conclusion

In conclusion, this paper has explored the critical theme of cybersecurity in the context of the Internet of Healthcare Things (IoHT). By investigating the Five Layers of the Concept of Cybersecurity, 5G security, Massive Machine Type Communication (mMTC), and Network Slicing, we have gained valuable insights into the challenges and measures associated with securing IoHT. Emphasizing the importance of proactive security in IoHT, the paper underscores the need for comprehensive strategies to safeguard patient data and ensure the integrity of healthcare systems. As technology evolves, ongoing research and collaboration are essential to stay ahead of emerging threats and fortify the resilience of interconnected healthcare environments.

6. References

[1] C.A. da Costa, C. F.Pasluosta, B. Eskofier, D.B. da Silva, R. da Rosa Righi, Internet of health things: Toward intelligent vital signs monitoring in hospital wards, Artif. Intell. Med. 89 (2018) 61–69, http://dx.doi.org/10.1016/j.artmed.2018. 05.005.

[2] S. Baker, W. Xiang, and I. ATKINSON, “Internet of things for smart healthcare: Technologies,” Challenges, and Opportunities,â IEEE, vol. 5, 2017

[3] S.M.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, K.-S. Kwak, The internet of things for health care: A comprehensive survey, IEEE Access 3 (2015) 678–708, http://dx.doi.org/10.1109/ACCESS.2015.2437951

[4] Ahmed, Mohiuddin, Surender Byreddy, Anush Nutakki, Leslie F. Sikos, and Paul Haskell-Dowland. "ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things." Ad Hoc Networks 122 (2021): 102621.

[5] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and privacy in iot-cloud-based e-health systemsâa comprehensive review," Symmetry, vol. 12, no. 7, p. 1191, 2020

[6] E.-C. Liou and S.-C. Cheng, "A qos benchmark system for telemedicine communication over 5g urllc and mmtc scenarios," in 2020 IEEE 2nd Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS). IEEE, 2020, pp. 24–26.

[7] T.-N. Chien, S.-H. Hsieh, P.-H. Cheng, Y.-P. Chen, S.-J. Chen, J.-J. Luh, H.-S. Chen, and J.-S. Lai, "Usability evaluation of mobile medical treatment carts: Another explanation by information engineers," Journal of medical systems, vol. 36, pp. 1327–1334, 2012.

[8] T. Hewa, G. GÃŒr, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," in 2020 2nd 6G Wireless Summit (6G SUMMIT), 2020, pp. 1–5.

[9] H. Jain, V. Chamola, Y. Jain, and Naren, "5g network slice for digital real-time healthcare system powered by network data analytics," Internet of Things and Cyber-Physical Systems, vol. 1, pp. 14–21, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345221000043.

[10] B. Dzogovic, T. Mahmood, B. Santos, B. Feng, V. T. Do, N. Jacot, and T. Van Do, "Advanced 5g network slicing isolation using enhanced vpn+ for healthcare verticals," in Smart Objects and Technologies for Social Good, I. M. Pires, S. Spinsante, E. Zdravevski, and P. Lameski, Eds. Cham: Springer International Publishing, 2021, pp. 121–135.

[11] E. M. Abounassar, P. El-Kafrawy, and A. A. Abd El-Latif, "Security and interoperability issues with internet of things (iot) in healthcare industry: A survey," Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions, pp. 159–189, 2022.

[12] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, and M. Iranmanesh, "The internet of things (iot) in healthcare: Taking stock and moving forward," Internet of Things, vol. 22, p. 100721, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660523000446.

[13] F. Nausheen and S. H. Begum, "Healthcare iot: Benefits, vulnerabilities and solutions," in 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 517–522.

[14] P. L. de Faria and J. V. Cordeiro, "Health data privacy and confidentiality rights: Crisis or redemption?" Revista Portuguesa de SaÃºde PÃblica, vol. 32, no. 2, pp. 123–133, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0870902514000352.

[15] M. Sookhak, M. R. Jabbarpour, N. S. Safa, and F. R. Yu, “Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues,” Journal of Network and Computer Applications, vol. 178, p. 102950, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520304045.

[16] S. Sachdeva and S. Bhalla, “Semantic interoperability in standardized electronic health record databases,” J. Data and Information Quality, vol. 3, no. 1, may 2012. [Online]. Available: https://doi.org/10.1145/2166788.2166789.

[17] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, “Identification and authentication in healthcare internet-ofthings using integrated fog computing based blockchain model,” Internet of Things, vol. 15, p. 100422, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660521000664.

[18] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, T. Lagkas, G. Fragulis, and A. Sarigiannidis, “A self-learning approach for detecting intrusions in healthcare systems,” in ICC 2021 – IEEE International Conference on Communications, 2021, pp. 1–6.

[19] N. Dissanayake, M. Zahedi, A. Jayatilaka, and M. A. Babar, “A grounded theory of the role of coordination in software security patch management,” in Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, ser. ESEC/FSE 2021. New York, NY, USA: Association for Computing Machinery, 2021, p. 793â805. [Online]. Available: https://doi.org/10.1145/3468264.3468595