Magna Scientia Advanced Biology and Pharmacy

eISSN: 2582-8363

Cross Ref DOI: 10.30574/msabp

Journal homepage: https://magnascientiapub.com/journals/msabp/

(REVIEW ARTICLE)

Check for updates

Security protocols in healthcare: A comprehensive study of AI-Enabled IoMT

Swetha Singiri [1,*], Naga santhosh reddy vootukuri [2] and Siri Chandana Katari [3]

[1] *Meta, Dallas, Texas, USA.*
[2] *Microsoft, USA.*
[3] *Department Computer Science & Engineering (IoT), Vasireddy Venkatadri Institute of Technology, Nambur, India.*

Magna Scientia Advanced Biology and Pharmacy, 2024, 12(01), 032–037

Publication history: Received on 24 March 2024; revised on 05 May 2024; accepted on 08 May 2024

Article DOI: https://doi.org/10.30574/msabp.2024.12.1.0030

Abstract

The Internet of Medical Things IoMT has driven a paradigm shift in the way things have been done traditionally within medical Healthcare practices and this is evidence that Smart Personal systems (Health Care) are shaping up with mighty forces. By merging these technologies, IoT has transformed data communication and provided the means to directly interconnect medical devices and sensor systems. The use of advanced technologies like Artificial Intelligence(AI), Machine Learning, Deep Learning, and Federated Learning has highly equipped and transformed the IoMT's performance. These integrations also raise concerns on data privacy and security, and addressing these challenges become more important as without proper security and privacy measures people can face serious disruption both online and offline leading to upcoming catastrophes already waiting at its end line. This chapter looks into the intricacies of a highly secure communications system powered by AI, specifically in the age where disasters like COVID-19 [10], emphasizes the need for increased security on data transmission as well as storage. IoMT has wide applications for integrating remote patient monitoring, enhancing user satisfaction and interdimensional hospitalization rates, we delve into how IoMT works in conjunction with machine learning, particularly federated Learning intends to address any possible concerns. The chapter begins with IoMT systems, including IoMT ecosystems, implantable medical devices IMDs, and Internet-worn gadgetry. Special attention is given to the AI-powered Intrusion Detection Systems (IDSs) in IoMT environments, while network security remains the research focus helping practitioners to implement safety measures enterprise-wide; analysis, comparison, and evaluation all encompass machine learning, deep learning mechanisms as precautions against potential attacks. We will also consider another study on the services of an AI-provisioned lightweight protocol communication system that ensures data authenticity and responds to diverse security implications in IMD. The chapter makes a U-turn by alluding to internet wearable devices, pointing out federated learning and blockchain reinforcements that indicate the need for an integrated framework. The amalgamation of future technologies supports the ethical and secure integration of IoMT. Collaboration, as a guiding principle, compels healthcare practitioners and policymakers to partner efficiently to guide the future where the security of health is ever easier. In the end, a summary of modern ethical and regulatory paradigms in IoMT is provided, emphasizing that there could be an urgent need for new laws.

Keywords: Internet of Medical Things; Internet of Healthcare Things; Federated Learning; Artificial Intelligence; Cybersecurity; Intrusion Detection System; ASCP-IoMT; Communication protocol Implantable; Internet Wearable Devices; Security protocols

1. Introduction

The synergy that has emerged largely from the integration of IoT with dynamic healthcare is referred to in terms of the Internet or Medical Things (IoMT). Within the personal domain of IoMT, a wide variety of devices ranging from activity trackers and heart rate monitors to smart clothing. These multiple tools have been engineered solely for user functions

* Corresponding author: Swetha Singiri

without direct medical intervention, under a specific regulatory regime on par with health-IoMT devices. The clinical IoMT devices, elaborately built to perform health monitoring with medical oversight can be defined as smart continuous glucose monitors or connected inhalers. The typical validation process is performed by manufacturers of these devices, carrying out clinical trials following the regulatory clearance process, thus can be used in clinics or in home settings. This categorization aims at presenting a complex vision of IoMT, conveying personalized and clinician-driven aspects in terms of health monitoring.

According to Caldwell et al. [3], Smart Healthcare can be classified into 4 ecosystem groups based on the IoMT devices, as shown in Fig. 1(a). The On-Body ecosystem can include IoMT devices such as wearables and implantable devices; In-Home ecosystems as devices like transportable medical equipment along with telemedicine present within the boundaries of a home. The In-Clinic ecosystem refers to devices used within the clinic settings like ambulatory care, while In-Hospital ecosystem involves devices like surgical tables and beds, ECG machines. In addition, there are four primary categories of medical devices/sensors: patient monitoring, implantable, environmental monitoring, and In-Hospital connected devices, as depicted in Fig. 1(b) [4], [5]. Finally, various healthcare applications have been distinguished by some researchers, as demonstrated in Fig. 1(c), including patient and environment monitoring, therapeutics, medical diagnosis, and workflow, which involves patients' surveillance, personal assistant platforms, patient and personal identification, and other activities. Some of the examples related to on-body IOMT are been discussed in the papers like [7][8]

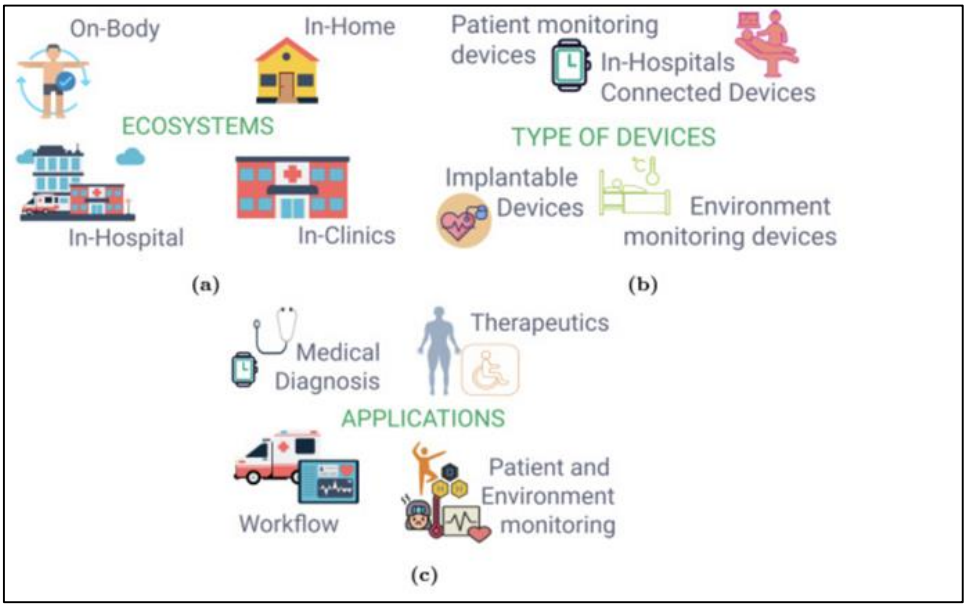

Figure 1[a][b][c] Patient monitoring, implantable, environmental monitoring, and In-Hospital connected devices

There is an increased need for all these ecosystems to seamlessly work together and integrate different disciplines, technologies to improve overall healthcare services. Finally, as shown in Fig. 1(d), the multidisciplinary application of medical healthcare application— patients data, therapeutics; medical diagnosis, device usage, workflow optimization etc is summarized with a broad view perspective. The users of these services or apps include patients who require monitoring and personal assistant platforms, patient identification, and personalized purposes in Smart Healthcare. [Link]

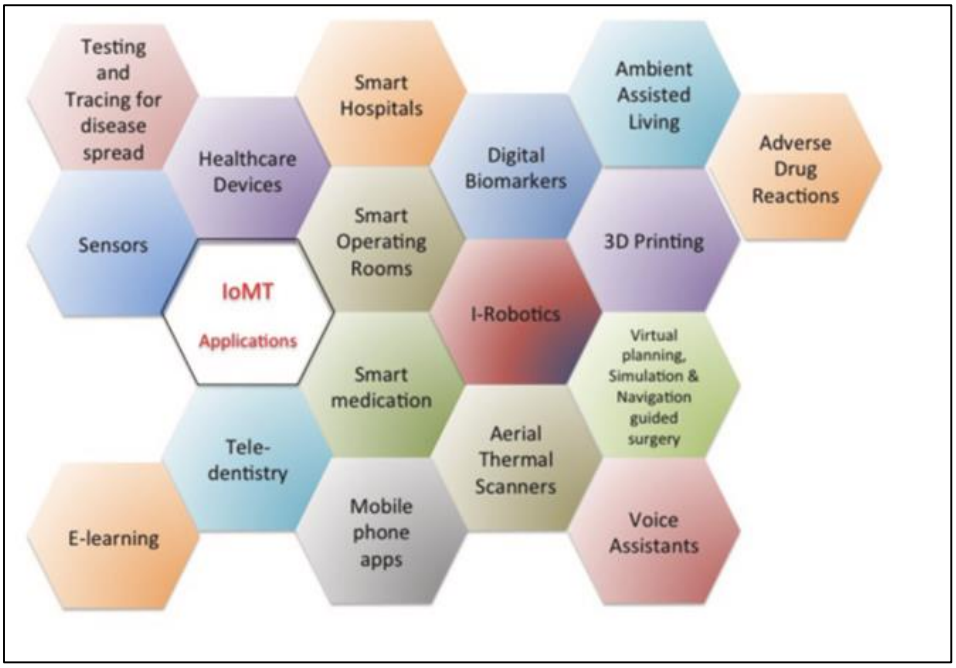

Figure 1(d) Multidisciplinary healthcare application [link]

2. Analysis of Internet of Medical Things Security Challenges

The digitization of the healthcare industry, enabled by medical device connectivity referred to as IoMT stems from a drive toward better patient and service outcomes. Nevertheless, this unification brings security threats that require thorough and thoughtful contemplation for the protection of individual patients' sensitive information; medical equipment itself, and the overall healthcare networks' safety. The major issue is about the exposure of IoMT devices to cyber risks, which include knowingly gaining access without permission to what we call unauthorized persons' entry into sensitive places like hospitals. Other threats are data breaches and malicious tampering. With the possible ramifications of such an attack on a healthcare system, especially if you take into consideration some breach in life-supporting equipment as mentioned by Hamilton and Rogers [98], protocols security along with bioinformatics and health data has now become drastically important. The most important security challenges to be addressed in IoMT include authentication, authorization process, data confidentiality protection availability, and integrity. The need for dealing with these issues is vital to guarantee IoMTs' capacity in terms of resilience and security when used in the realm of healthcare should be emphasized.

3. Artificial intelligence for IoMT security - Intrusion Detection Systems

More than twenty years ago, various Incidence Detection Systems (IDS) were recognized as an integral part of network and element protection. The purpose of IDS is to proactively detect unauthorized access, security breaches and provide real-time alerts to improve overall security. However, the traditional IDS methods applied to IoMT have distinctive challenges due to its properties such as limited-resource devices specific for system protocol standards and stacks that constrain all these parameters. This section provides an overview of the study which is aimed at the IoMT network carried out by IDS research efforts. Several studies have been performed in recent years on IoMT IDS. Fig 2(a) shows different techniques and datasets discussed in various surveys. The comparison in this table discusses the contributions of each survey related to the develop intrusion detection system for IoT. Axelssons research on intrusion detection systems and taxonomy (Axelsson, 2000) categorized intrusion detection systems based on their methods of detection. The highly cited survey by Debar et al. (Debar et al., 2000) surveyed detection methods based on the behavior and knowledge profiles of the attacks. A taxonomy of IoT intrusion systems by Liao et al. (Liao et al., 2013a), has presented a classification of five subclasses with an in-depth perspective on their characteristics: Statistics-based, Pattern-based, Rule-based, State-based and Heuristic-based. The classification we make for IDSs is carried out on a basis of attributes like detection approach, validation approach and as well placement strategy among others. Specifically, none of these surveys cover all detection methods of IoT, which is considered crucial because of the heterogeneous nature of the IoT ecosystem. The variety in the IoT IDS surveys indicates that a study of IDS for IoT must be reviewed. Specifically, none

of these surveys cover all detection methods of IoT, which is considered crucial because of the heterogeneous nature of the IoT ecosystem.[Link]

Survey	Intrusion Detection System Techniques							Attacks on IoT	Validation Strategy	Deployment Strategy	IoT Dataset
	SIDS	AIDS					Hybrid IDS				
		Supervised	Unsupervised	Semi-supervised	Ensemble methods	Deep Learning					
Lunt (Lunt, 1988)	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
Axelsson (Axelsson, 2000)	✔	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖
Liao, et al. (Liao et al., 2013b)	✔	✔	✔	✖	✖	✖	✔	✖	✖	✖	✖
Agrawal and Agrawal (Agrawal & Agrawal, 2015)	✔	✔	✔	✔	✔	✖	✔	✖	✖	✖	✖
Buczak and Guven (Buczak & Guven, 2016)	✔	✔	✔	✖	✔	✖	✔	✔	✖	✖	✖
Zarpelao, et al. (Zarpelao et al., 2017)	✖	✔	✔	✖	✖	✖	✖	✔	✔	✔	✖
Khraisat, et al. (Khraisat et al., 2019a)	✔	✔	✔	✔	✔	✔	✖	✖	✖	✖	✔

Figure 2(a) IDS techniques and datasets covered by the surveys

4. Artificial intelligence enabled lightweight protocol for IoMT

The Lightweight High-Security cryptographic scheme for Human Service systems controlled by the IoT platform is another recent AI-inspired light communication network developed in 2015 and designed to solve problems brought on due to changes of the environment (IoMT). The architecture aims to provide secure communication among implantable devices, personal servers, and cloud server plans using robust authentication in conjunction with a key setup process. This also brings a comprehensive analysis of the network model and threat model, where in-depth information about an arrangement of devices as well as users within IoMT are given along with details regarding threats to information security related to the fields somehow connected. To justify ASCP-IoMT's relevant resilience against both passive and active attacks, a case study is conducted in which the system runs several security assortments: eavesdropping/intercepting channels; and relay attack models. But the results solidify the scheme's security posture. Moreover, a comparison between ASCP-IoMT and similar models is given to achieve better results by IOMT. An IoMT environment suffers from different security and privacy related issues because it can be attacked through various methods. Under the presence of these attacks, the sensitive health data can be leaked or altered. Therefore, we need a strong security mechanism to mitigate these attacks in IoMT. Hence, a new AI-enabled secure communication protocol for an IoMT environment has been presented. The discussed network and threat models of the proposed ASCP-IoMT provided the details of the arrangements of various network devices and the associated attacks of the IoMT. The conducted security analysis proved the security of ASCP-IoMT against various potential attacks. During the comparative performance analysis, it has been observed that the proposed ASCP-IoMT provides better security with additional functionality as compared to existing similar techniques. [Link]. Ofcouse with AI there come many areas to cover like regulations

5. Blockchain-based federated learning methodologies for IoMT

Ensconced under the umbrella term IoMT, a healthcare network of portable medical equipment has been charged with harvesting highly detailed datasets on a person-level basis. Such data files are confidential in nature and size; they should therefore be stored and managed from a secured environment. Perhaps led by the promise offered, cryptographic elements find application in healthcare technologies that are based on blockchain, and going forward; this trend is likely to grow. Although it is the blockchain network that has great fame due to its stable and decentralized nature, tamper-proofing, wisdom of immutability treaty about agreeableness trait as data prone ability, confidentiality when done by anyone. This technology plays a significant part in solving the following issues: data manipulation prevention, integrity maintenance, and secured access to storage areas as well as distributed computation on decentralization of local objects. In this paper, we propose a resilient medical data processing and storage system that applies blockchain technology to protect client information from malicious tampering. To diffuse the issues of security and privacy, we use federated learning. As far as medical use is concerned, connect in one word—such an amalgamation of machine learning and blockchain has been investigated even though with very rare success. This hook, especially used in federated learning, makes it possible to remote procedures and analyses without the transmission of strictly protected personal health information. The principal goal is to boost the performance of healthcare services and, consequently, increase people's quality lives using IoMT technological implementations. [Link]

6. Simulation and analysis of IoMT security challenges

The vulnerability of IoMT devices to both newly discovered attacks arises from reasons, due to the absence of established security measures during device manufacturing significantly increasing their risks. Moreover the nature of these devices and the setup of networks worsen security issues, because the different types of network protocols used at each level poses a challenge as a one size fits all security solution may not be effective for all. Estimates from Statista suggest a rise in the number of devices in the European Union (EU) projected to reach 25.8 million devices by 2025. This growth along with the increase in the number of smart medical devices combined with affordable wireless sensors highlights the importance of addressing security and privacy concerns (He et al., 2018). As this continues to grow the amount of data generated is also expected to increase (Dimitrov, 2016; Firouzi et al., 2018; Ma et al., 2017), possibly reaching 79.4 zettabytes by 2025 (O'Dea, 2020). Sun, Lo & Lo (2019) recently conducted a study on security and privacy of IoMT focusing on security requirements and challenges and more focus on authentication and access control (Sun, Lo & Lo, 2019). Additionally, a detailed survey on the IoMT security and privacy was performed by Newaz et al. (2020), where a detailed analysis was performed on current solutions for healthcare IoT security. Alternatively, a review on the IoMT security issues and challenges about the attacks and their impact on the IoMT was presented, with special focus on lightweight security solutions (Yaacoub et al., 2020). Hence, traditional security measures and approaches pose a significant risk to healthcare sensitive data, and there is an immediate need for leveraging innovative technological advancements. [Link]

7. Conclusion

According to the Washington Post, in 2020 17% of the U.S. population had people aged 65 and over and is expected to grow from 55.7 million to 80.8 million by 2040, a growth of 45% (link). Considering that this group of people will have an increased need for medical treatments, this signifies that a huge portion of the US population have a need for medical assistance and it's critical to establish ethical and regulatory paradigms. Currently we have several regulatory agencies to protect data privacy and security- FDA, HIPAA, Federal Communication Commission (FCC), Federal Trade Commission (FTC), but they have their own limitations and loopholes. FDA has established data security and privacy guidelines in IoMT, but it is only applicable to limited devices and it also has failed in enforcing the guidelines efficiently. HIPAA is primarily applicable to in-clinic and in-hospital devices, but doesn't cover On-Body wearables like Fitbit. This can have potential data leak risks. On the other hand, FCC is primarily focused on handling radiation damage, while FTC is focused on protecting consumer data collected through IoMT devices. The IoMT market is expected to grow significantly to meet the increased demands of connected medical devices and data sharing, and there is an urgent need to address the current limitations and challenges, and keep up the pace with technological advancements to avoid data leakage, cybersecurity threats and other security concerns. Instead of having disparate regulatory agencies, there is a need for a central authority responsible for establishing and enforcing guidelines. Any new law established needs to be enforced on existing devices already being used in the market, along with new devices to avoid any potential data leak. This requires partnering closely with all healthcare agencies like institutions, third-party organizations, diagnostics, pharmaceuticals etc, beyond geographical boundaries to address all the loop-holes efficiently. In conclusion, there is an urgent need for establishing new laws to address this rapidly evolving landscape focusing on key ethical and regulatory considerations.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest

References

[1] Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain ISSN:2315-4462 (jocm.us)

[2] Mazhar T, Talpur DB, Shloul TA, Ghadi YY, Haq I, Ullah I, Ouahada K, Hamam H. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. Brain Sci. 2023 Apr 19;13(4):683. doi: 10.3390/brainsci13040683. PMID: 37190648; PMCID: PMC10136937.

[3] M. Elhoseny et al., "Security and Privacy Issues in Medical Internet of Things: Overview Countermeasures Challenges and Future Directions", Sustainability, vol. 13, no. 21, pp. 11645, Oct. 2021.

[4] Y. Rbah et al., "Machine Learning and Deep Learning Methods for Intrusion Detection Systems in IoMT: A survey," 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, 2022, pp. 1-9, doi: 10.1109/IRASET52964.2022.9738218.

[5] A. Meena, G. M. V. Reddy and D. P. Chavali, "Accelerated CNN Training with Genetic Algorithm," 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 2024, pp. 1-6, doi: 10.1109/IATMSI60426.2024.10502992.

[6] keywords: {Training;Technological innovation;Machine learning algorithms;Sociology;Machine learning;Robustness;Convolutional neural networks},

[7] Bhatt MW, Sharma S. An IoMT-Based Approach for Real-Time Monitoring Using Wearable Neuro-Sensors. J Healthc Eng. 2023 Feb 13;2023:1066547. doi: 10.1155/2023/1066547. PMID: 36814546; PMCID: PMC9940964.

[8] G. Thamilarasu, A. Odesile and A. Hoang, "An Intrusion Detection System for Internet of Medical Things", *IEEE Access*, vol. 8, pp. 181560-181576, 2020

[9] https://doi.org/10.30574/wjarr.2024.22.1.1251

[10] Chavali, Durga, Vinod Kumar Dhiman, and Siri Chandana Katari. "AI-Powered Virtual Health Assistants: Transforming Patient Engagement Through Virtual Nursing."

[11] Durga Chavali, Biju Baburajan, Ashokkumar Gurusamy, Vinod Kumar Dhiman, Siri Chandana Katari, Regulating Artificial Intelligence: Developments And Challenges, Int. J. of Pharm. Sci., 2024, Vol 2, Issue 3, https://doi.org/10.5281/zenodo.10898480

[12] P. Kumar, G. P. Gupta and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks", Comput. Commun., vol. 166, pp. 110-124, Jan. 2021.

[13] A. A. Hady, A. Ghubaish, T. Salman, D. Unal and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study", IEEE Access, vol. 8, pp. 106576-106584, 2020.

[14] https://www.doi.org/10.55041/IJSREM31544

[15] Meghana, G.V.R., Chavali, D.P. and Meghana, G.V.R., 2023. Examining the Dynamics of COVID-19 Misinformation: Social Media Trends, Vaccine Discourse, and Public Sentiment. Cureus, 15(11).