Journal of Trends in Computer Science and Smart Technology (ISSN: 2582-4104)
www.irojournals.com/tcsst/

Future Challenges of the Internet of Things in the Health Care Domain - An Overview

S. Smys[1], Jennifer S. Raj[2]

[1]Professor, Department of Electrical and Electronics Engineering, RVS College of Engineering and Technology, Coimbatore, India
[2]Professor, Department of ECE, Gnanamani College of Technology, Namakkal, India

E-mail: [1]smys375@gmail.com, [2]jennifer.raj@gmail.com

Abstract

Medical IoT systems have recently become one of the most sophisticated medical technologies in well-developed countries. The remote monitoring of medical services may benefit greatly from this technology. According to a new study, security measures and training are critical in protecting IoMT systems from cyber-attacks. In this paper, the primary security and privacy challenges with IoMT are examined using current security solutions. Non-cryptographic and cryptographic approaches are used for a variety of attacks. It's therefore possible to compare the computational complexity of the various solutions and the resources they demand. Besides, the discussion of attack versions with causes for possible solutions, the dangerous scenarios of various attacks are also provided here. IoMT security methods, particularly in the rapidly expanding field of digital healthcare, show a trade-off between security level and system performance. There is a final section that talks about the acceptable security solutions, such as various attacks through common solution methods and protocols.

Keywords: IoMT, health care, cyber-attacks, medical devices, medical sensor, healthcare unit

1. Introduction

The advent of numerous technologies has resulted in technology integration being an intrinsic part of our everyday lives. The IoT plays a vital role in facilitating smooth and seamless ubiquitous services for everyone by reducing the amount of human effort required. Networking physical things that are smart and networked, as well as sensors, software, and network connections, are referred to as the Internet of Things (IoT) in general. IoT is now altering and changing the corporate and consumer sectors, and it is making its way into almost every industry on the planet. In addition, it is used in a wide range of other sectors, including healthcare, smart cities, agriculture, and the military, among others [1-5].

DOI: https://doi.org/10.36548/jtcsst.2021.4.003
Received: 21.12.2021, received in revised form: 13.01.2022, accepted: 30.01.2022, published: 09.02.2022

A new era in health care has dawned due to the invention of medical gadgets. With the advancement of technology, need to visit the hospital on a daily basis is no longer required to keep tabs on our health. Even though this drastic change is greatly appreciated, we must take a step back and evaluate the security of these devices [7, 8].

These gadgets' safety and privacy are in jeopardy. When it comes to securing medical gadgets, the implications may be catastrophic, since many patients' lives are at stake. The significance of patient safety in healthcare cannot be overstated. People's everyday lives are made simpler for those in the healthcare profession thanks to the growing expansion and adoption of IoT applications in numerous disciplines and industries. Devices feature a wearable sensor, actuators and other add-ons that link to communicate easily over the Internet [9, 10]. There are, however, serious security issues and hazards associated with these IoMT apps that use the Internet.

Thus, IoT systems need a solid security foundation based on a comprehensive understanding of security for all IoT parts at all levels. Unavoidable medical services are seen as creative solutions to worldwide medical issues because of the growing demand for excellent medical services and the increasing cost of treatment. The IoMT was sparked in part by advancements in the Internet of Things. Precautionary care may be shifted from the current focus on cost and avoidance, but the protection issues of these sensing frameworks are often overlooked. To ensure the safety of the patient, medical equipment and their interactions must be clearly visible [11].

1.1 Internet of Medical Things (IoMT)

The IoT useful insights can only be gleaned by linking, diverse people and objects in a healthcare business or healthcare ecosystem, to each other. Connecting patients, doctors, and other healthcare professionals is a typical use case in this industry. Many relevant health initiatives have been launched by healthcare organizations, with a focus on including patients and the public in the process. Consumers and patients are encouraged to adopt healthier choices, which will result in reduced healthcare expenditures and achieve better results. Monitoring patients' vital signs and activities and keeping them responsible for their healthcare choices would further encourage compliance. There is an increasing emphasis on improving the health of people in order to reduce healthcare expenditures throughout the world [12-14]. Remote patient monitoring has been made possible by a greater emphasis on consumer interaction and novel techniques to integrate IoT-based IoMT technology, such as personal

digital assistants, accessible to the patient, with intelligent medical equipment. Thanks to this new technology, medical providers may have a better grasp of a patient's health and the expenses connected with their treatment. Figure 1 contains various medical sensors for entire IoMT architecture [15].

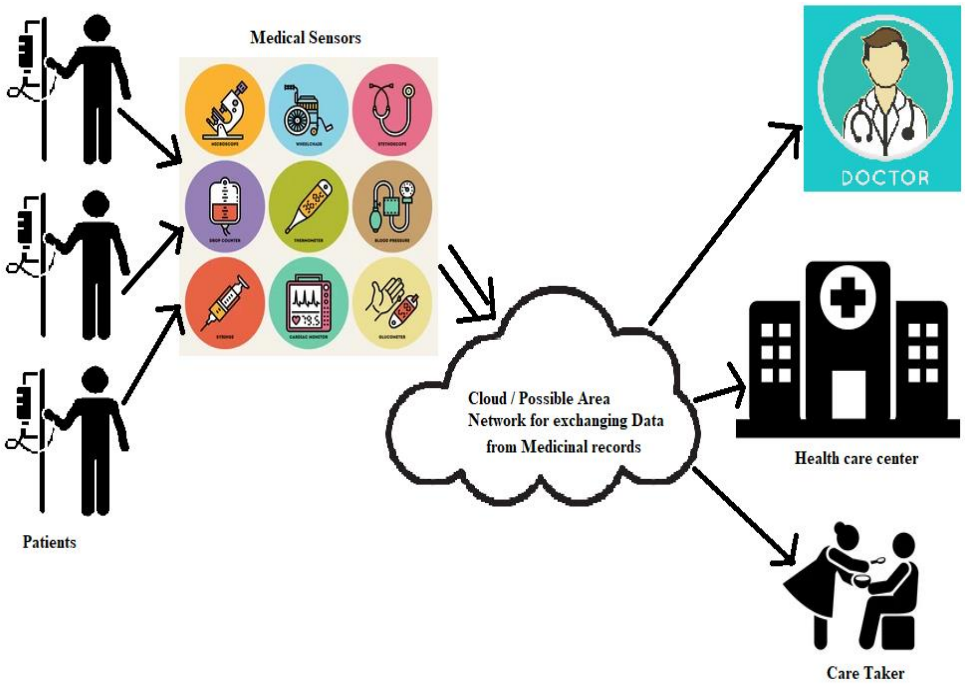

Figure 1. Internet of medical things architecture

1.2 Organization of the Research

The following is the layout of this research article: Section 3 provides a review of the literature on medical device and sensor integration with possible existing attacks, followed by a discussion of the idea. Section 4 delves further into the topics of privacy and security in the Internet of Things. Section 5 depicts potential future attacks on the IoMT as well as its classification of possible solution. Last but not least, it finishes with suggestions for potential future study fields.

2. Literature Survey

Medical devices and biosensors, such as those used by Dang et al., captured and transmitted large volumes of raw biological data in real time, including heart rate, brain activity, body temperature, and blood glucose level [16]. To save the first records of a patient, Newaz and coworkers suggested that personal servers often feature a computational structure

that is connected with the cloud storage database. Furthermore, the patient is alerted if an irregularity is detected by the device's warning system [17].

A passive or active attack on the IoMT, is identified as the one that threatens the secured privacy, as described by Sun, Lo, and other authors. The influence on the IoMT system's security needs was also considered when classifying prospective attacks based on the IoMT targeted layer. Finally, despite the recorded incidents, zero-day attacks might still occur on a regular basis. These attacks not only jeopardize the privacy of patients, but also cause enormous financial loss and harm to their image [18].

In light of the rising threat of cyber-attacks on the IoMT system, it has become necessary to create and build effective security solutions. Supervised, unsupervised, and semi-supervised machine learning methods may be used to address the security concerns of the Internet of Things. According to Meidan et al., the supervised method used data that has already been assigned a class or label. Classification and regression are two types of supervised learning. Support vector machines, decision trees, and neural networks are examples of supervised learning. Signature-based intrusion detection systems employ these techniques to identify attacks and malware. Unsupervised approaches, on the other hand, group data based on similarities rather than differences, since human labelling of data is not always straightforward [19].

In IoMT, Gupta et al., addressed machine learning approaches for identifying new attacks and demonstrated how adversarial assaults on machine learning techniques may be avoided by using semi-supervised models for attack detection. In addition, new assaults on network theory showed that not all unlabelled data are useful for prediction. As a result, tagged data may be used to get around this problem. There is a recent machine learning branch called semi-supervised learning in which, part of the learning data are annotated [20].

Deep Learning (DL), a new field of machine learning, has recently evolved, which is an improved type of neural network. For object detection, voice recognition, language translation, and decision-making, it uses a multi-layered artificial neural network that mimics the human brain's basic functioning principles.

3. Security and Privacy of IoMT

There is a risk of classic and zero-day attacks on the IoMT devices. To a large extent, this is due to the absence of security standards and controls that are now in place for IoT

network devices and their production. Due to the limited computing power and battery life of small devices, cryptography and other advanced security measures cannot be implemented. A single security solution may not work on all devices since the IoMT's network is made up of multiple protocols at each tier. The IoMT system defines the following metrics with security and privacy concern:

3.1 Authentication

All IoT devices must be able to identify and verify each other. As a result, the authentication procedure may not be available. In this way, the data and reading devices are protected against unauthorised access, modification, deletion, or injection. Attempts to tamper with the integrity of an implanted pacemaker, for example, may result in death. When a service needs data, computational resources, or communications, this system makes sure that they are always available and functioning properly [21-25]. In a surgical room outfitted with wireless medical equipment, a system outage presents a risk to patients' health. When it comes to the Internet of Things, it's possible to connect a wide range of various devices that have variable features or capabilities and release dates and versions.

Table 1. Application domain for security and privacy

S.No	Security and privacy	Application
1	Authentication	Healthcare, protection against common attack
2	Confidential	Healthcare, Continuous monitoring without disturb
3	Entire Management System (EMS)	Healthcare, User interfacing

3.2 Confidential

Confidentiality is regarded as one of the most important aspects of security. Security and privacy necessitate that only authorized individuals have access to private information. As a result, IoT users may be divided into a number of different subgroups, such as humans, machines, services, internal objects, and non-networked things. With regard to interacting with users or procedures involving user data, confidentiality is essential. It ensures that private

information is protected from unwanted access. Data leaks and even life-threatening scenarios might occur as a result of unauthorized access.

3.3 Entire Management System (EMS)

EMS must make sure that data is properly managed, protected, and sent while utilising IoT technology. In order to do this, a variety of regulations and standards must be implemented. A means for enforcing such regulations on organisations to adhere to global standards must also be taken into account. The transmission of certain encryption materials between IoT devices and sensors, necessitates the employment of easy-to-use systems to manage their keys that are capable of creating trust and distributing keys across various devices without requiring a high degree of skill [26].

Open communication channels and a disregard for data privacy make it very likely that secret and private information may be leaked, hacked, or compromised. Passive or aggressive assaults, both have the potential to undermine this. An activity metric measures how well a system can confirm the existence or absence of a certain activity. As a result, it assures that both the sender and recipient nodes get a delivery receipt and verification of the sender's identity.

4. Future Attacks in IoMT

The attacks are intended for obtaining sensitive information from the node network. There are two types of attacks.

- Active attack
- Passive attack (Monitoring / Eavesdropping).

Wireless access points are scanned by passive eavesdropping to discover what medical equipment is linked to them. Passive eavesdropping is the opposite of active eavesdropping, in which an adversary listens in on data transmissions [27]. This data is then used for the collection of far more accessible and speedier information. Typical medical records, for example, may be scanned. IoMT healthcare security threats are discussed elaborately in this section.

4.1 Active Attack

Table 1 shows possible attacks against future attack version. Besides, this section discusses some of the active attack types.

4.1.1 Capturing of Medicinal Records (CMR)

This is one of the most dangerous attacks because it allows one adversary to intercept data and pass it along to another. It is possible that an assault of this kind may lead to physicians making incorrect judgments that could hurt patients by tampering with the data in transmitted messages.

4.1.2 Install Virus Data in Records (IVDR)

The system is hacked by creating a legal entity that can provide access to the system. The attacker stops a genuine user's communication and then injects the erroneous message into the system. IoMT systems are severely impacted as a consequence of this attack, which may result in the death of patients by producing message containing false information and distributing it to physicians and the hospital's databases. A hacker impersonating an honest backup server in the system causes a bogus update to be presented by the unfair script system. The consequence is that the IoMT devices may be accessed and tailgated without authorization.

4.1.3 Network Jam by Fake ID (NJFID)

Wi-Fi networks are one of the main intended targets for this type of attack. As a result of the attacker's actions, patients and hospitals are unable to contact one another. Fake requests and information are used in these assaults in an effort to overwhelm the medical system and drain its resources [28].

4.1.4 Disabling Medicinal Record (DMR)

IoMT connections using Transmission Control Protocols (TCPs) for communication between the doctor's system and the patient's system are common targets for this attack. Web servers and email are examples of this record of medicinal data. By using the e-healthcare server's stored memory in order to enable a connection that is not safe from a future assault, these methods aim to disable medical servers.

Table 2. Possible solutions against attack version

S.No	Attack Versions	Causes	Danger for	Solutions
1	Capturing of Medicinal Records	*Exploits IoMT vulnerability*	Healthcare domain,	*Robustness to the Local Area Network*

			Patient's routing tablets	
2	Install Virus Data in Records	*Security network attack*	Collapsing of Medicinal Record	*Appropriate antivirus installation*
3	Network Jam	*Host finding and attack*	Network collapsing for IoMT devices	*Clear network issues by congestion control*
4	Disabling Medicinal Record	*Reading devices and acquiring data for modification*	Hide medicinal data records for further treatment	*Password Protected*
5	Remote Access	*Access weak passwords*	Continuous monitoring	*Password protected*
6	Damage of IoMT Devices	*Exploits nodes connection in the network*	All sensors and devices damage	*Frequent node examination*
7	Accessing Medicinal Records	*Remote access through weak password*	Eavesdrops	*Strong password protection*

4.2 Passive Attacks

Patients and medical staff are prevented from listening in on local area networks by an internet control message protocol assault on the target central processor unit of a computer network.

4.2.1 Remote Access of Medicinal Records (RAMR)

Attempting all potential passwords, this attack aims to identify the one that works. If the medical records or patient credentials need to be accessed, it is requisite to break down every term that can be thought of. Patients' remote medical sensors are not the only ones targeted by this attack.

4.2.2 Damage of IoMT Devices (DID)

The striker uses the knots node to relocate the wireless network for a variety of nefarious reasons. The first problem is that it repeatedly sends false alerts on medical emergency alarms. The provision of medical services for patients at a hospital might be affected by this assault. Control signals supplied to other medical equipment may be altered or tampered with by an attacker who can signal the system [29]. By routing information to another site, attackers may intercept and steal it. The IoMT devices' immune systems may be damaged as a result of this.

4.2.3 Accessing Medicinal Records (AMR)

Medical systems are vulnerable to this assault if an IoT device's security procedures aren't rigorous enough. Dictionary terms are used to guess passwords in these attacks. Many people depend on weak hashes since two passwords may have the same hash. Because of this vulnerability, the hacker has unauthorized access to the medical systems. Among malware, this is the most harmful and destructive. Using a linked device, they may self-reproduce and exploit the device's weaknesses. The medical staff may have to keep their hands full dealing with these attacks.

5. Conclusion

IoT services and technology in healthcare are discussed in this article. A number of new research issues that will likely become important study directions in the next few years have been selected. Several important research advantages and the most significant application domains have also been discovered. It is anticipated that this study will assist medical academics and practitioners in gaining a better understanding of the IoT's potential in the medical field and the considerable hurdles it faces. Researchers as well will get a better understanding of IoT applications in healthcare as a result of this effort. It is true that the Internet of Medical Things (IoMT) is vulnerable to a variety of threats and concerns that primarily aim to compromise patient privacy and the confidentiality, integrity, or accessibility of medical services. However, among the issues, difficulties, and limitations faced by IoMT examined in this study, several security methods that may be used to protect and secure the IoMT domains and their related assets, including medical equipment and systems have been analysed.

References

[1] Sharma, R. Rajesh. "Design of Distribution Transformer Health Management System using IoT Sensors." Journal of Soft Computing Paradigm 3, no. 3 (2021): 192-204.

[2] Harshal Arbat1, Srishty Choudhary2 & Kumkum Bala, "IOT Smart Health Band", Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-5, 2016. ISSN: 2454-1362

[3] Shakya, Subarna. "A Self-Monitoring and Analyzing System for Solar Power Station using IoT and Data Mining Algorithms." Journal of Soft Computing Paradigm 3, no. 2 (2021): 96-109.

[4] Pallavi Chavan , Prerna More, Neha Thorat, Shraddha Yewale & Pallavi Dhade, "ECG - Remote Patient Monitoring Using Cloud Computing", Imperial Journal of Interdisciplinary Research (IJIR) Vol-2,Issue-2 , 2016 , ISSN : 2454-1362

[5] Chen, Joy Iong Zong, and Lu-Tsou Yeh. "Graphene based Web Framework for Energy Efficient IoT Applications." Journal of Information Technology 3, no. 01 (2021): 18-28.

[6] Boyi Xu, Lida Xu, Hongming Cai, Lihong Jiang, Yang Luo & Yizhi Gu, "The design of an m-Health monitoring system based on a cloud computing plat form", Talor & Francis 2015. doi: 10.1080/17517575.2015.1053416

[7] Rahimunnisa, Dr K. "LoRa-IoT Focused System of Defense for Equipped Troops [LIFE]." Journal of Ubiquitous Computing and Communication Technologies 2, no. 3 (2020): 153-177.

[8] Liaqat, S., Akhunzada, A., Shaikh, F. S., Giannetsos, A., & Jan, M. A. (2020). SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT). Computer Communications, 160, 697-705.

[9] Patil, Prachu J., Ritika V. Zalke, Kalyani R. Tumasare, Bhavana A. Shiwankar, Shivani R. Singh, and Shailesh Sakhare. "IoT Protocol for Accident Spotting with Medical Facility." Journal of Artificial Intelligence 3, no. 02 (2021): 140-150.

[10] Wazid, M., Das, A. K., Rodrigues, J. J., Shetty, S., & Park, Y. (2019). IoMT malware detection approaches: analysis and research challenges. IEEE Access, 7, 182459-182476.

[11] Mugunthan, S. R. "Soft computing based autonomous low rate DDOS attack detection and security for cloud computing." J. Soft Comput. Paradig.(JSCP) 1, no. 02 (2019): 80-90.

[12] Wazid, M., Das, A. K., Rodrigues, J. J., Shetty, S., & Park, Y. (2019). IoMT malware detection approaches: analysis and research challenges. IEEE Access, 7, 182459-182476

[13] Joe, C. Vijesh, and Jennifer S. Raj. "Deniable Authentication Encryption for Privacy Protection using Blockchain." Journal of Artificial Intelligence and Capsule Networks 3, no. 3 (2021): 259-271.

[14] Chen, F., Luo, Y., Zhang, J., Zhu, J., Zhang, Z., Zhao, C., & Wang, T. (2018). An infrastructure framework for privacy protection of community medical internet of things. World Wide Web, 21(1), 33-57.

[15] Dang LM, Piran M, Han D, Min K, Moon H. 2019. A survey on internet of things and cloud computing for healthcare. Electronics 8(7):768 DOI 10.3390/electronics8070768.

[16] Newaz A, Sikder AK, Rahman MA, Uluagac AS. 2020. A survey on security and privacy issues in modern healthcare systems: attacks and defenses. Available at https://arxiv.org/abs/2005.07359.

[17] Sun Y, Lo FP-W, Lo B. 2019. Security and privacy for the internet of medical things enabled healthcare systems: a survey. IEEE Access 7:183339–183355 DOI 10.1109/ACCESS.2019.2960617.

[18] Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, Elovici Y. 2018. N-BaIoT-network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing 17(3):12–22 DOI 10.1109/MPRV.2018.03367731.

[19] Gupta R, Tanwar S, Tyagi S, Kumar N. 2020a. Machine learning models for secure data analytics: a taxonomy and threat model. Computer Communications 153(5):406–440 DOI 10.1016/j.comcom.2020.02.008.

[20] Bashar, Abul, and S. Smys. "Physical Layer Protection Against Sensor Eavesdropper Channels in Wireless Sensor Networks." IRO Journal on Sustainable Wireless Systems 3, no. 2: 59-67.

[21] Wong, A. M. K., Hsu, C. L., Le, T. V., Hsieh, M. C., & Lin, T. W. (2020). Three-Factor Fast Authentication Scheme with Time Bound and User Anonymity for Multi-Server E-Health Systems in 5G-Based Wireless Sensor Networks. Sensors, 20(9), 2511.

[22] Balasubramaniam, Vivekanadam. "IoT based Biotelemetry for Smart Health Care Monitoring System." Journal of Information Technology and Digital World 2, no. 3 (2020): 183-190.

[23] Yan, X., Geng, T., & Ding, H. (2014). Efficient cryptographic access control protocol for sensitive data management. Journal of Computers, 9(1), 222-228

[24] Raj, Jennifer S. "Secure Data Sharing Platform for Portable Social Networks with Power Saving Operation." Journal of IoT in Social, Mobile, Analytics, and Cloud 3, no. 3 (2021): 250-262.

[25] Kumar, BR Arun. "Impact of Cyberattacks on Electronic Patient Health/Medical Records." In Computer Networks and Inventive Communication Technologies, pp. 885-898. Springer, Singapore, 2021.

[26] George, Anjana, Anu S. Alunkal, Gopika G. Nair, and Poornasree R. Mohan. "Privacy Protection and Con Dentiality in Medical IoT." In International Conference on Computer Networks and Inventive Communication Technologies, pp. 21-27. Springer, Cham, 2019.

[27] Moharana, Meena, Siddharth Swarup Rautaray, and Manjusha Pandey. "A Survey on Big Data Solution for Complex Bio-medical Information." In International Conference on Computer Networks and Inventive Communication Technologies, pp. 229-237. Springer, Cham, 2019.

[28] Chidambaram, Nithya, Kona Sai Harshavardhan Reddy, Keertipati Vishal Varma, Kakamani Jagadeesh Sai Dheeraj, Avija Sharan Reddy, and Amirtharajan Rengarajan. "Tamper Detection of Medical Images Using Modified Hashing Algorithm." In International Conference on Intelligent Computing, Information and Control Systems, pp. 491-498. Springer, Cham, 2019.

[29] Kumar, JR Dinesh, C. Ganesh Babu, V. R. Balaji, K. Priyadharsini, and S. P. Karthi. "Performance investigation of various sram cells for iot based wearable biomedical devices." In Inventive Communication and Computational Technologies, pp. 573-588. Springer, Singapore, 2021.

Author's biography

S. Smys received his M.E. and Ph.D. degrees in Wireless Communication and Networking from Anna University and Karunya University, India. His main area of research activity is localization and routing architecture in wireless networks. He serves as Associate Editor of Computers and Electrical Engineering (C&EE) Journal, Elsevier, and Guest Editor of MONET Journal, Springer. He served as Reviewer for IET, Springer, Inderscience and Elsevier journals. He has published many research articles in refereed journals and IEEE conferences. He has been General chair, Session Chair, TPC Chair and Panelist in several conferences. He is Member of IEEE and Senior Member of IACSIT wireless research group. He has been serving as Organizing Chair and Program Chair of several International conferences and in the Program Committees of several International conferences. Currently, he is working as Professor in the Department of Information Technology at RVS technical Campus, Coimbatore, India.

Jennifer S. Raj received the Ph.D degree from Anna University and Master's Degree in communication System from SRM University, India. Currently she is working in the Department of ECE, Gnanamani College of Technology, Namakkal, India. She is a life member of ISTE, India. She has been serving as Organizing Chair and Program Chair of several International conferences, and in the Program Committees of several International conferences. She is book reviewer for Tata Mc Graw hill publication and publishes more than fifty research articles in the journals and IEEE conferences. Her interests are in wireless Health care informatics and body area sensor networks.