ISSN 2278-3091
Volume 10, No.6, November - December 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse061062021.pdf
https://doi.org/10.30534/ijatcse/2021/061062021

Malware Detection Approaches and Analysis for the Internet of Medical Things Enabled Healthcare Systems

Mohammad Sirajuddin[1], Dr.B Sateesh Kumar[2]
[1]Research Scholar, Department of Computer Science & Engineering JNTU, Hyderabad, Telangana, India, mohdsiraj569@gmail.com
[2] Professor, Department of Computer Science & Engineering JNTUH-College of Engineering, Jagtial, Telangana, India, sateeshbkumar@jntuh.ac.in

Received Date : October 10, 2021 Accepted Date : November 09, 2021 Published Date : December 06, 2021

ABSTRACT
The advancement of information and communications technology has changed an IoMT-enabled healthcare system. The Internet of Medical Things (IoMT) is a subset of the Internet of Things (IoT) that focuses on smart healthcare (medical) device connectivity. While the Internet of Medical Things (IoMT) communication environment facilitates and supports our daily health activities, it also has drawbacks such as password guessing, replay, impersonation, remote hijacking, privileged insider, denial of service (DoS), and man-in-the-middle attacks, as well as malware attacks. Malware botnets cause assaults on the system's data and other resources, compromising its authenticity, availability, confidentiality and, integrity. In the event of such an attack, crucial IoMT communication data may be exposed, altered, or even unavailable to authorised users. As a result, malware protection for the IoMT environment becomes critical. In this paper, we provide several forms of malware attacks and their consequences. We also go through security, privacy, and different IoMT malware detection schemes.

Key words: IoMT, Malware Detection, Privacy, IoT Security.

1. INTRODUCTION

Internet of Medical Things (IoMT) is used for a variety of applications in healthcare. Patients are continuously monitored in healthcare using network of sensors and actuators, and data can be stored in cloud infrastructure. By patient monitoring equipment with many sensors, a medical expert can understand, identify the problem, and offer patients solutions via the cloud. In some circumstances, a high-level application can analyse data independently and give both parties recommendations or alarms. IoMT is a term used in the health sector to describe this interconnected medical equipments. Portable low-power embedded microcontroller units (MCUs), sensors, and actuators make up the majority of IoMT nodes. IoMT components do not have sophisticated security safeguards against cyberattacks to keep prices low; consequently, it is critical for designers to properly assess their security levels. The use of IoMTs is growing extremely fast, and by the following decade, the number of biosensor devices has surpassed 50 billion. Security of healthcare network infrastructure and associated IoMT devices is a severe challenge in this regard.

The healthcare network infrastructure uses a large and diverse set of related equipment and services to save lives. These are resource-constrained gadgets with limited security capabilities that can be easily compromised. Patients' privacy may be compromised due to eavesdropping, and life-threatening episodes may be missed due to the disruption of the regular functioning of IoMT devices caused by DoS assaults[1]. Due to their low power and processing capability, many security methods cannot be used with IoMT devices. Compared to ordinary IoT devices, implantable and wearable medical and healthcare devices are generally developed with lower computing power and energy capacities since they must be shrunk in size. IoMT devices must store and process personal health data, and some even include actuation features to assist users in maintaining their health. As a result, IoMT devices are projected to have substantially greater security requirements than traditional IoT and computer devices[3].

On the other hand, security and priacy are frequently disregarded in the design of IoMT healthcare systems. Most biosensor equipment is designed to communicate and store information on the internet for processing and analysis. This advancement in healthcare systems facilitates medical experts to respond to patients being monitored by medical and healthcare equipment more quickly and precisely. However, it increases the risk of user data being abused or stolen while kept on cloud servers. The privacy of users' data, particularly personal data, must be safeguarded. In addition to devising assault countermeasures, post-attack procedures must also be carefully examined. Financial data, such as credit card security codes, may be rapidly rendered invalid and useless, while personal health information might expose a person's present health status[3]. When this information is stolen due to a security breach, retrieving and eradicating the stolen information is both difficult and crucial. Substantial restrictions and severe punishments from governments and healthcare organizations are required to secure patient data.

2. IOMT BASED HEALTHCARE SYSTEM ARCHITECHTURE

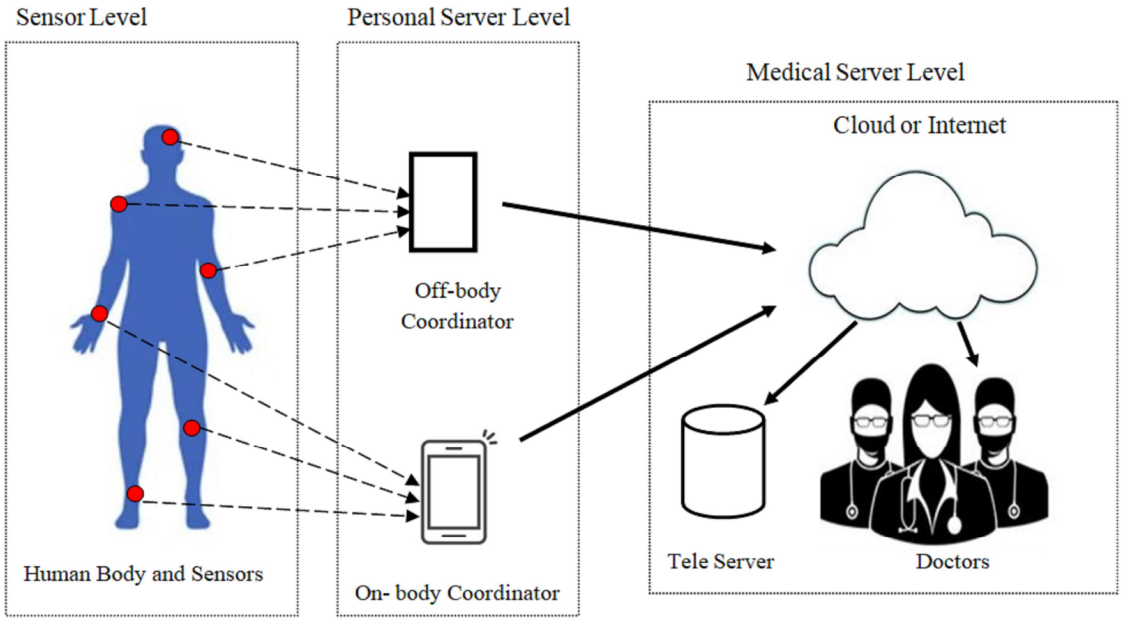

Fig 2.1 IoMT-based healthcare systems Architecture

IoMT-based healthcare systems have the following phases: Sensing phase, Personal Server phase, and Medical server phase, as shown in Fig.2.1. IoMT environments have used this architecture. Many recently suggested IoMT-based healthcare systems. The sensor level contains medical equipment and sensors that form a local body Sensor Network (BSN) [3]. In the sensor and personal server levels, less-power wireless methodology protocols such as Near-Field Communication(NFC), Bluetooth, and RFID are frequently used for wireless communications. RFID and NFC can enable significantly fewer energy communications, commonly required by implantable devices, but BLE allows several network topologies, including star and mesh. Medical information is gathered by medical equipment and transmitted to personal servers. Personal systems process and store patient data locally before sending it to centralized medical servers[3]. When the network connection to the medical servers is disrupted, a personal server must function normally. Medical workers, such as doctors, have remote access to patients' data and provide timely advice. IoMT-based healthcare systems have been developed in recent years for continuous patient monitoring. However, many do not include any security or privacy protections in their designs or are left as future work.

.

3. IOMT HEALTHCARE SYSTEM SECURITY AND PRIVACY REQUIREMENTS

Healthcare systems based on IoMT have more stringent privacy and security requirements than standard IoT-based infrastructures. Many different security needs for IoMT healthcare systems exist, such as device localization, which can help secure the systems' security and privacy. Each level of the IoMT healthcare system has different functionalities, which means that each level has different security and privacy requirements. As a result, each level's criteria are examined and described separately[3]. Security and privacy requirements for the IoMT healthcare systems are classified into the following levels

1. Data level security requirements
2. Sensor level security requirements
3. Personal Server level security requirements
4. Medical Server level security requirements

3.1 Data Level Security Requirements

Confidentiality

Only authorized persons should have access to patient health data collected and stored according to ethical privacy rules. Appropriate steps must be taken to safeguard the confidentiality of health data linked with specific patients to prevent data breaches. The necessity of such safeguards cannot be overstated, as data obtained by cybercriminals may be sold on black markets**,** putting patients at risk of privacy violations and financial and reputational harm[3].

Integrity

The data integrity requirement for IoMT healthcare systems is designed to ensure that data arriving at the intended destination has not been tampered with in any manner during wireless transmission. Attackers might take advantage of the wireless network's broadcast feature to access and change patient data, which could have severe ramifications in

life-threatening scenarios. It is critical to detect any illegal data distortions or alterations to ensure that the data has not been compromised. As a result, appropriate data integrity measures must be created to prevent malicious attempts to modify sent data. Furthermore, the integrity of the data stored on medical servers must be ensured, which implies that the data cannot be readily tampered with[3].

Availability
When services and data are required, they must be made available to the relevant users. When DoS attacks occur, medical servers and devices' services and data become inaccessible. Any unavailable data or services might lead to potentially fatal scenarios, such as the failure to give timely notifications in the case of a heart attack[1]. As a result, to account for the risk of data loss, healthcare apps must be accessible at all times to users and emergency services.

3.2 Sensor Level Requirements

Security and privacy at the sensor level are the most difficult parts of the three-tier IoMT healthcare system due to the low processing capabilities and power limits of medical devices and sensors.

Localization
IoMT upholds two types of sensor restriction: on-body sensor position and sensor/patient arrangement in an indoor setting. The main sort of sensor confinement is used to build up whether or not the sensors are in the appropriate body places. Sensor restriction, frequently known as Location of Things (LoT), is the method involved with finding a sensor in a room or a patient wearing a sensor in an office. Due to the idea of IoMT medical care frameworks, clinical gadgets might relocate all through network inclusion on a routine basis[3]. A continuous interruption identification approach is required if the organization's sensors leave and rejoin at capricious spans.

Self-Healing
After the network attacks, IoMT devices resume operating. An IoMT system should identify and diagnose assaults and apply appropriate security procedures with little human interaction to accomplish self-healing[2]. Self-healing solutions should be as light as possible regarding network communication overheads and processing complexity for medical and healthcare devices.

Forward And Backward Compatibility
Forward and Backward compatibility is a must in real-time healthcare applications, where damaged medical sensors must be replaced as soon as possible. Medical sensors cannot read future signals if they are transmitted after the sensors have left the network, which is known as forwarding compatibility. On the other hand, backward compatibility means that messages sent previously cannot be read by a sensor that has just joined the network[3].

Tamper-Proof Hardware
IoMT devices, particularly ambient sensors, can be physically stolen, exposing security information to attackers. Furthermore, attackers can reprogramme the stolen devices and reinstall them in the system, listening to communications without being detected. As a result, medical device theft is a serious security problem addressed in IoMT healthcare systems[3]. Medical equipment in the systems should at the very least contain tamper-resistant integrated circuits, which prohibit third parties from reading codes placed on the devices once they have been installed.

3.3 Personal Server Level Requirements

Patients' data is frequently kept and aggregated on personal servers before being transferred to medical servers in IoMT healthcare systems. Therefore ensuring that the data is securely safeguarded while on the personal servers is critical. Personal server-level security maintenance has two types of authentication schemes: device authentication and user authentication.

Device Authentication
Before accepting data from medical devices and sensors, the personal server must complete authentication. For data security and integrity, the device authentication mechanism should establish secured/encrypted communications. Device authentication is reciprocal between personal servers and devices, but because personal servers often have more excellent computational capability and power than medical devices and sensors, most of the computation should be done on them.

User Authentication
Before accepting data from medical devices and sensors, the personal server must complete authentication. For data security and integrity, the device authentication mechanism should establish secured/encrypted communications. Device authentication is reciprocal between personal servers and devices, but because personal servers often have the more excellent computational capability and power than medical devices and sensors, most of the computation should be done on them.

3.4 Medical Server Level Requirements

According to two of the most significant criteria for the security and privacy of patient data at the medical server level, only authorised devices and employees have access to the data, and the data itself must be encrypted at all times while stored in databases. As more paper-based medical records are transferred to electronic medical records (EMRs), concerns concerning the security and privacy of medical servers that contain EMRs are becoming more prevalent[3]. As a result, appropriate IoMT healthcare system security measures must be implemented at the medical server level.

Access Control
Effective access control measures must be installed to guarantee that only authorised devices and employees have access to the medical servers. Because obtaining a patient's permission or consent every time a data access request is made is difficult, medical server service providers should provide patients with selective access control, allowing patients to choose which data can be shared without permission and which third parties can have access[2].

Trust Management
The term "trust" refers to two-way interaction between two reliable data-sharing nodes, such as a sensor node and a network coordinator. trust is defined as the degree to which a node feels safe and reliable while dealing with another node. Wireless healthcare applications require widespread collaboration across network nodes to be successful. Trust management systems may be used to detect a node's level of trust in this respect, which is significant since trust evaluation of a node's behaviour, such as data delivery and quality, is critical in healthcare applications.

Resistance To Dos Attacks
Jamming, Node Tampering, Spoofing, Homing etc., are the most prevalent denial-of-service (DoS) threats against wireless healthcare applications. High-energy signals, such as jamming assaults in the physical layer [6], can be used by attackers to prevent the wireless network from functioning correctly. Many ways to safeguard and self-repairing the network against such attacks, such as evasion defence and competition strategies, have been presented, but they are all still in the early stages of development. Because of wireless networks' mobile and dynamic nature, more research is needed to create solutions to secure real-time IoMT healthcare systems from DoS assaults.

Key Management
To develop secure applications, basic administration moves toward executing and conveying cryptographic keys to sensor hubs are fundamental. Trusted server and key pre-circulation are the two fundamental key administration strategies utilized in IoMT medical care frameworks. Trusted server conventions accomplish significant organization understanding in a confided base station. Although these conventions are appropriate for progressive organizations, they are unsatisfactory for basic applications, for example, those identified with medical care since a complete organization disappointment may deliver a confided server in an ongoing situation inoperable[4].

4. TYPES OF MALWARE

Malware is a program generally distributed over the internet that steals, infects, or does other malicious operations directed by the attacker. The malware allows the attacker to use an infected system via remote control. It spreads other malware from the afflicted computer to other computers. It looks into the infected user's local network to conduct more malware attacks. Different Malware types which can attack IoMT devices of health care systems are described below

Spyware
It's a type of malware that monitors user activity without their permission. Malicious actions such as keylogging, activity tracking, and data harvestings, such as account passwords and financial data, such as credit card information, are possible in the network. It may potentially change the software's security settings. It takes advantage of software flaws and attaches itself to a regular program.

Trojan Horse
This malware acts like an authentic program to delude individuals into downloading and introducing it. It empowers a programmer to acquire remote admittance to a contaminated framework with authorization. When programmers approach a tainted framework, they can take delicate data (for example, financial information account number and Mastercard number). It can likewise introduce other malignant projects in the framework, doing other ruinous demonstrations.

Adware:
It's also known as an ad-supported program (software). As part of its functioning, it automatically distributes adverts. Pop-up advertisements on websites are a famous example of adware[5].

Ransomware
It usually spreads via downloaded files or other vulnerabilities in the operating system or networking software and demands payment from its owner (ransom)[3].

Rootkit
It is a kind of noxious programming that is very damaging. A rootkit can be utilized by programmers to remotely get to (control) a framework (e.g., an IoT gadget) without being identified by the client or security apparatuses. When introduced, the programmer can remotely execute records, take significant information, change framework designs, and modify the activity of safety programming. Because of its secret nature, recognizable proof and counteraction are incredibly difficult[3].

Mirai
Mirai is a type of malware that allows remote bots to control network devices running the Linux operating system. These devices can be used as part of a botnet to carry out more widespread malicious assaults. It is aimed primarily at smart IoT devices, such as Internet-connected consumer electronics[6].

Reaper
In comparison to the Mirai botnet, it can corrupt smart IoT devices very quickly. It also has other serious consequences, as it can quickly bring down the entire system [3]. The attacker might potentially use this botnet to modify the malware code to make it more dangerous.

5. MALWARE DETECTION SCHEMES IN IOMT ENABLED HEALTH CARE SYSTEMS

5.1 Blockchain-Based Malware Detection Scheme

The blockchain's operations can be utilized to protect a variety of communication contexts. Because blockchain activities are decentralized, efficient, and transparent, this is the case. Blockchain techniques may also be utilised to identify malware efficiently in the IoT/IoMT context. Using this detection technique, we may add a block to the blockchain containing information on malicious programs (i.e., malware)[7]. Because the blockchain is available to all authorised parties, these parties can learn about the system's current malware assaults.

5.2 Cross-Platform Malware Detection

When we want to establish a malware detection system, the heterogeneity of IoT networks causes difficulty. This attribute makes it easier to connect different application domains. However, it complicates the development of a reliable malware detection system. When a smart home application receives data from a healthcare monitoring device, the malware detection approach must be compliant and robust so that the program may access the data from the target network without difficulty. [2]. At the same time, it's worth noting that data saved in the cloud necessitates robust virus detection and prevention systems.

5. 3 Machine Learning-based Malware Detection Method

Installing a malware detection system in the IoMT environment is crucial for keeping the environment free of malicious activities. The raw network traffic intercepted by the sniffing equipment is stored in the first database. The second database is a collection of past datasets that show the network's profile history. The third database contains fresh signatures of discovered malware assaults and updates the second database regularly. The processing of a big volume of data needs more resources and a longer processing time[2]. As a consequence, the raw data files in database one are converted into colour pictures using the pre-processing data module. The colour pictures obtained from the pre-processing data module are delivered to the detecting module. The detection module learns from signatures in the database[8]. If the given data does not match the signatures in the database, it is deemed an attack.

5.4 Deep Learning-based Malware detection Method

The Deep Learning-based Malware identification Method is divided into five stages. During the input phase, the training pictures are sent into the neural network. In the first place, the convolution step enhances signal qualities and reduces noise. Second, by retaining critical data, the pooling stage reduces the amount of data processing. The completely connected phase in the third stage turns the two-dimensional feature into a one-dimensional element and delivers it to the classifier. Fourth, the dropout phase controls the problem of data over-fitting. Finally, the classifier categorizes the malware images[9].

6. CONCLUSION

IoMT-based healthcare applications make our lives easier. However, IoMT healthcare devices are very prone to security threats. In the IoMT context, it is critical to provide effective and efficient security solutions for malware attacks. IoMT healthcare systems have more stringent security and privacy requirements than standard IoT-based infrastructures because of their low energy, low bandwidth, and low processing power. In this paper, we discussed security and privacy requirements for IoMT enable health care devices. We are also investigated numerous types of malware and their detection methods in this work.

REFERENCES

1. W. Zang and Y. Li, "Gait-cycle-driven transmission power control scheme for a wireless body area network," IEEE J. Biomed vol. 22, no. 3, pp. 697_706, May 2018.
2. M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," in *IEEE Access*, vol. 7, pp. 182459-182476, 2019, doi: 10.1109/ACCESS.2019.2960412.
3. Y. Sun, F. P. -. Lo and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," in *IEEE Access*, vol. 7, pp. 183339-183355, 2019, doi: 10.1109/ACCESS.2019.2960617.
4. Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," Inf. Sci., vol. 479, pp. 567_592, Apr. 2019
5. X. Cheng, Z. Zhang, F. Chen, C. Zhao, T. Wang, H. Sun, and C. Huang, "Secure identity authentication of community medical Internet of Things," IEEE Access, vol. 7, pp. 115966_115977, 2019. .
6. S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. Yoon, and K. Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," IEEE Access, vol. 5, pp. 3028–3043, 2017.
7. R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, "A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features," IEEE Access, vol. 7, pp. 64 411–64 430, 2019
8. Naeem, Hamad 2019/10/01 Detection of Malicious Activities in Internet of Things Environment Based on Binary Visualization and Machine Intelligence Wireless Personal Communications
9. Kallol Krishna Karmakar, Vijay Varadharajan, Uday Tupakula, Surya Nepal, Chandra Thapa." Towards a Security Enhanced Virtualised Network Infrastructure for Internet of Medical Things (IoMT)", 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020