# THE INTERNET OF MEDICAL THINGS (IOMT): SECURITY THREATS AND ISSUES AFFECTING DIGITAL ECONOMY

**Conference Paper** · January 2021

DOI: 10.1049/icp.2021.2420



**3 authors**, including:

Azhar Ghafoor
COMSATS University Islamabad
**3** PUBLICATIONS **18** CITATIONS

SEE PROFILE

# THE INTERNET OF MEDICAL THINGS (IOMT): SECURITY THREATS AND ISSUES AFFECTING DIGITAL ECONOMY

***Mudassar Mushtaq, Munam Ali Shah, Azhar Ghafoor***

*Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan*
*mudassarmushtaqganai@gmail.com, mshah@comsats.edu.pk, azharghafoor39@gmail.com*

**Keywords:** IMOT, MALWARE, RANSOMWARE, SPOOFING, REPLAY ATTACK

## Abstract:

In the healthcare industry, we cannot deny, contradict or oppose the importance of the Internet of Medical Things (IoMT). The ultimate purpose of the IoMT system is to gather and transmit health information such as ECG, weight, blood pressure and sugar levels. Such data may be shared with an approved individual, who may be a physician, a participating health company, insurance provider, or an external contractor regardless of their time, location, and device. But the story is not as simple because IoMT faces various emerging cyber-attacks and threats. Day by day new malware attacks are created and launched on IoMT because an attacker knows that this market is worth billions. The purpose of writing this paper is to introduce you to some of the well-known attacks that are launched on IoT. Such as denial of service, router attack, sensor attack, repay attack, fingerprint, and time-based spoofing, and recent malware attacks such as like Miari, Emoted, Gamut and NE curs and ransomware in IOMT.

## 1. Introduction

The Internet of Things (IoT) is an ever-changing technological paradigm that links billions of smart objects to intelligent ecosystems such as smart grids, smart health, smart homes, smart factories, smart cities, smart vehicle networks, and the Industrial Internet of Things (IoT). The recent Industrial IoT revolution is currently rising enormously, resulting in immense monetary benefits and efficiency [1]. But prevalent and open environment increases the chances for an attacker to attack and exploit IoMT devices [2]. The diverse and dynamic nature of IoT devices open the door for cyber threats and attacks that lead to different assaults like distributed denial of service (DDOS), distributed attack data injection advance and long-lasting threat and attack and worse malware botnet intrusion that can breach your confidentiality and availability or even destroy your system [3].

IoMT is thus vulnerable to numerous emerging cyber threats such as identity theft, keylogging, phishing, and malicious bot as well data management and storage problems and exchange of data between nodes [4]. Resource limitations, scalability, distribution, mobility and low latency are also the main issues that give a chance to attackers to attack [5]. Data is usually transmitted with the help of a wireless medium. As a result it increases the chances of vulnerabilities because data is transferred through the air so an attacker can easily sniff the packet if no encryption or security mechanism is used [6]. Privacy and security are the main issue because the patient did not want to share their personal health issues, but data can even be lost by accidental [7]. As a result, data encryption and authentication are the burning issues in communication between channels over a public network [8].

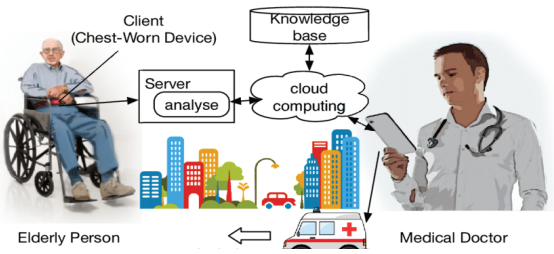


Fig. 1 Health monitoring scenario of IoMT devices

Look at fig 1 to show that a person sitting in a wheelchair has a different sensor that is used to gather information because many people are alone at home and do not have access to a hospital. They can communicate with their doctor or hospital with the help of IoMT and in case of emergency, a doctor can prescribe him first aid and alert the ambulance. But the case is not over; intruders can temper the data, spread false information about a patient, fake or mislead the emergency call as a result it can cause a worse effect on patient health.

## 2. Literature review

In this section, we highlight different opinions, processing function, author research, and their methods regarding security and emerging threats in IoMT.

IoT medical devices produce a large amount of data which is very difficult to manage and store. As a result, it is difficult to maintain the privacy and security of client health information. The priority of the patient is that their privacy should not be breached at any cost because they may not want to share details of diseases like HIV (human immunodeficiency virus) or psychiatric with society. Many upgrading algorithms like (AES), (DES), (RSA), and cipher encryption policies were used to enhance the security but failed due to the enormous size of data. Additionally, health care data has many hazards due to many factors such as insider curiosity, accidental disclosure, insider activity, unauthorized access, and physical intrusion. For better data security and efficiency, three sensors are used. Their purpose is to send their data to a mobile after that immune artificial system is used on the information which is gathered from the sensor. Its purpose is to normalize and train data just according to its memory cell and pool. Then data is further examined with a spiral search after which figures that are not matched are exempt from it because it will be considered a threat [7].

With the help of an artificial neural network a new authentication-based security scheme is introduced in which finger ECG is used to authenticate a user in the healthcare environment rather than old-fashioned security procedures such as password, face, and fingerprints. The ECG signal cannot just be intercepted, duplicated, and continuously identified. Fifty aspects were continually examined during this process, in which ECG was obtained with the aid of a mobile device. A neural network is used to process the data using exploratory screening. An algorithm can authenticate a user within three seconds, which is considered a good authentication system. Only 10% of the error rate comes out against the conventional methods. An efficient biometric design was used by the device to significantly improve security performance and accuracy in the healthcare industry [9].

As we know due to the dynamic and miscellaneous nature of IoT devices they are very vulnerable to attack by malware botnets. For the deduction of the botnet, a solution is proposed in which hybrid DL-driven (software-defined networking) is used to detect the malware botnets. The solution is cost-effective, adaptive, and flexible. To begin, the solution is implemented via SDN's control panel, which is simple to configure and provides critical centralized intelligence. Second, it ensures that the IoMT devices are not overloaded. By comparing this solution to other algorithms, it is demonstrated that it produces superior results [1], [10].

IoMT and IoT devices usually work on the three-layer principle of application, network, and perception. The perception layer purpose is to get data from actuators and sensors and collect, detect, and process information and send it to the network layer. Then the network layer function is to transmit data on different devices like a hub with the help of the internet. The goal of the application layer is just to fill the CIA cycle with confidently, authenticity and integrity. To ensure a good security mechanism, four points are discussed as follows. Software running on all IoT devices should be certified. When an IoT computer is switched on, it can first authenticate to the network before capturing or transmitting data. It should first authenticate itself to the network when an IoT device is turned on before collecting or sending data. The IoT network needs firewalling for packet filtering, which is directed to the devices because IoT devices have limited processing and memory resources. Patches should be periodically updated, so there is no additional bandwidth usage. The current state of IoT research focuses predominantly on protocols for authentication and access control, but with the rapid development of technology, new networking protocols such as IPv6 and 5G need to be implemented to accomplish the complex mashup of IoT geometry [11].

For better communication between devices, we need a good approach that can compensate for vulnerabilities, attacks and threats. To provide good and effective security in IoMT deceives the analytic network process is used with ISO/IEC standard. It consists of three components: goal, criteria and alternatives [12], [13].

The basic purpose of IoMT is to provide facilities regarding time and place but, due to wireless connectivity, it is more vulnerable and different types of attacks such as sensor attack, replay attack, time-based spoofing, denial of service (Dos) attack and forwarding attack are common now [6]. The Internet of Medical Things (IoMT) is a built-in sensor, wearable appliance, medical device, and clinical system ecosystem that offers the ability to respond

quickly and improve the quality of treatment for various medical applications such as remote monitoring of the healthcare system [14]. Current technologies can provide patient data protection to a certain degree during data transfer, but cannot stop certain advanced threats and assaults, such as collaboration attacks and data disclosure.

We then suggest a functional system called Privacy Protector, the data collection for patient privacy secured to avoid such attacks. Privacy Protector protects hidden sharing and shares repair suggestions for patients' privacy (in the event of data loss or compromises). We use numerous cloud server distributed networks to ensure the confidentiality of patients' private details as well as one of the servers remains uncompromised. We also have a control scheme for patient access, where multiple cloud servers work together to provide patients' data to health care providers without exposing data information [15].

### *2.1 Taxonomy diagram of attacks*

In figure 2 we draw a taxonomy diagram that focuses on types of attack that further extend into their origin, difficulty, types and level.

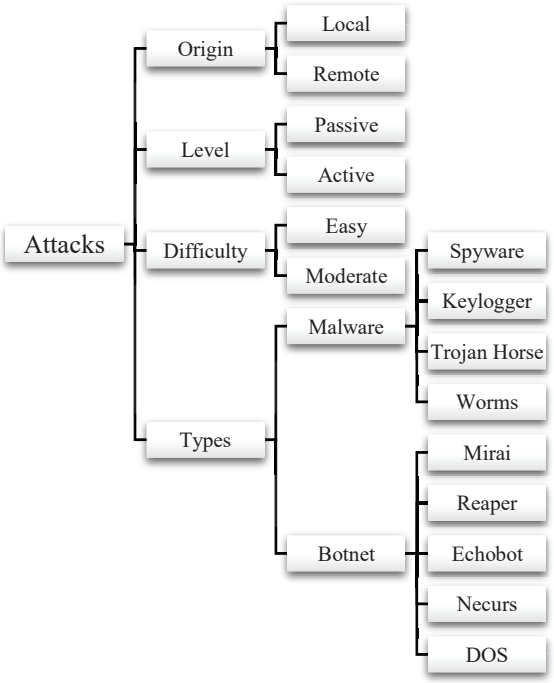


Fig 1 Taxonomy of attacks and threats of IoMT

### *2.2 Comparative Table*

In this section, we compare the different techniques, proposed solutions, and algorithms. The main objective of this comparative table is to check whether it is a cost-effective solution and which principle of CIA is breach or focus.

Table 1 Comparative table of the different proposed solutions.

| Algorithm | Result | Confidentiality | Integrity | Availability | Cost-Effective |
|---|---|---|---|---|---|
| Hybrid DL-Driven and SDN | Accuracy 99% | ✓ | × | × | × |
| Provide useful information about attacks and their prevention | | × | ✓ | × | ✓ |
| Spiral swarm optimized | Accuracy 97-98% | ✓ | ✓ | ✓ | × |
| Denny bilinear pairing-based scheme | | ✓ | ✓ | × | × |
| Discuss the three layers of IoMT application, network, and perception | | ✓ | ✓ | × | ✓ |
| Evaluating security in IoMT | | × | × | ✓ | × |
| Privacy protected | Accuracy 94.9% | × | × | ✓ | ✓ |
| SW-SSS | | × | ✓ | ✓ | ✓ |
| Provide solution for device-level security | Risk 95% | × | × | × | ✓ |
| RF | Accuracy 99.67 | × | ✓ | ✓ | × |

## 3. Future trends, assaults, safeguards, and threats to IoT/IoMT

IoT/IoMT is broadly used in every field of the world from a small house to huge corporations. However, due to its vulnerable nature, it can easily be exploited by attackers. Therefore, new challenges are revolving around the security of IoT/IoMT devices. We need to examine cyber threats and design a new and effective security protocol as a matter of our health cannot be compromised.

As we know, health is wealth. According to a Deloitte report worldwide, health expenditure is forecast to expand from $7.1 trillion in 2015 to $8.7 trillion by 2020 because adults aged 65 or older nearly doubled by 2050. The global demand for IoMT could increase from $41 billion in 2017 to $158 billion dollars by 2022. A graph is constructed, using data from Deloitte, to predict that importance of the IoMT devices is such that its market will be boosted by three times within the five years. New types of pandemics hitting the world will only increase tend

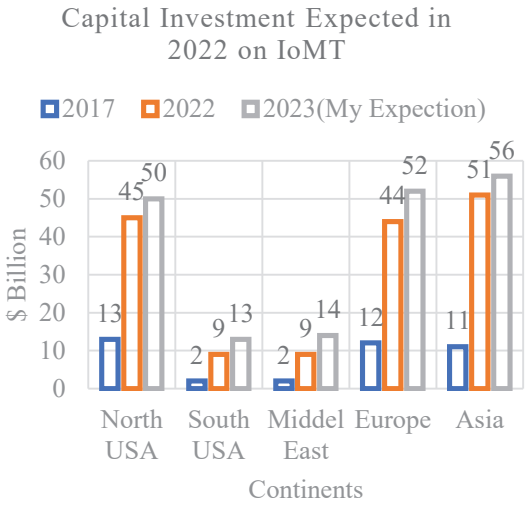


Fig. 3 Future capital investment in IoMT.

But attackers are also becoming more intelligent day by day, practicing very hard, finding vulnerabilities, making new botnets to launch DDoS attacks, and lots more. So, it is an wake-up call for all of us: if we are not able to provide full proof security to IoMT devices then the billion-dollar industry will have no future. Day by day the number of IoT/IoMT devices grows exponentially more than 9.9 billion IoT/IoMT devices present in the world. So, what number can it reach in a few numbers of years?

We can estimate the value by analyzing the current growth of devices. Figure no 3 predicts the growth of IoMT devices with the help of the trend line. This is taken from the Laptrinx blog website

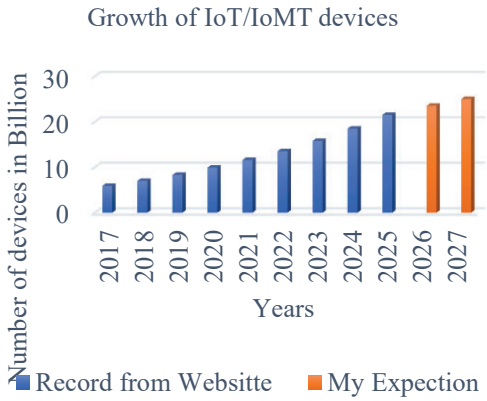


Fig 4: Calculating growth factor of IoT/IoMT devices

By analysing the figure 4, the exponential growth of is clear because day by day we are getting more and more accustomed to automation and dependent on gadgets. As a result, the number of devices will also increase. But as the number of devices increases the number of attacks and vulnerabilities also increases.

The risk of a ransomware attack is now one of the greatest obstacles that IoT is facing. The effects, including loss of confidential data, reduced performance, data degradation, negative publicity, and health monitoring downtime are catastrophic. Downtime in the health industry can lead to patient death. Available data and statistics on this significant attack need to be reprocessed to educate scientists and professionals. Below I construct a bar graph that illustrates how much money the world lost from the ransomware attack.

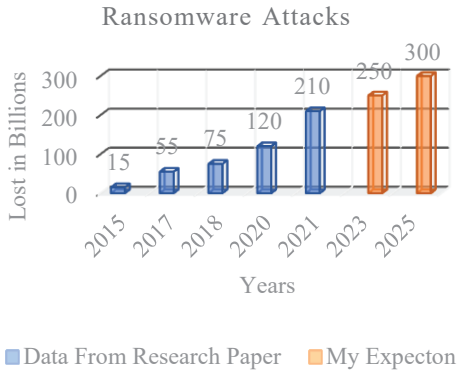


Fig. 5 money lost by the world from a ransomware attack.

## 4. Conclusion

By 2025, more than 21 billion IoT/IoMT devices are expected to exist due to more demand, and the world is moving towards smart city, smart health monitoring. IoT/IoMT systems are useful for daily life. However, internet connectivity still poses an intrinsic danger for all IoT/IoMT users. The truth is clear that everything related to the internet is prone to cyber-attacks. As a result, cyber-attacks are in danger of becoming an avalanche. Cyber-criminals use IoT/IoMT to promote attacks like DDoS and ransomware. The world is moving towards more artificial intelligence and its use in health monitoring by identifying habits and lifestyle and suggesting changes. 5G will keep fuelling IoT/IoMT growth networks, Major telecommunications networks are starting to introduce 5G networks and ensuring fast speed up and connecting of IoT/IoMT devices simultaneously in billions. Developed countries are increasingly considering the big issue that is patient or client policy and making new laws and policies to protect people's data. In short, we can say that a fight has started between two: one is an attacker and the other is a victim. The attacker tries its best to destroy the victim, and the victim tries its best to stop an attacker. The winner is the one who works hard to find their loophole and update himself with modern tactics

## 5. References


[1] Liaqat, T.,Akhunzada, A., F.Shaikh., et al., "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)," Comput. Commun., vol. 160, no. July, pp. 697–705, 2020, doi: 10.1016/j.comcom.2020.07.006.

[2] Makhdoom, I., Abolhasan,. J.Lipman.,et al., "Anatomy of Threats to the Internet of Things," IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1636–1675, 2019, doi: 10.1109/COMST.2018.2874978.

[3] Sisinni, E.,Saifullah, S. Han, U. Jennehag,.et al., "Industrial internet of things: Challenges, opportunities, and directions," IEEE Trans. Ind. Informatics, vol. 14, no. 11, pp. 4724–4734, 2018, doi: 10.1109/TII.2018.2852491.

[4] Prajoy Podder, P. K. P. , M., Rubaiyat Hossain Mondal, Subrato Bharati, "Review on the Security Threats of Internet of Things," Int. J. Comput. Appl., vol. 176, no. 41, pp. 37–45, 2020, doi: 10.5120/ijca2020920548.

[5] Chaudhary, R.,Aujla, G. S., S. Garg, N. Kumar, and Rodrigues J. J. P. C., "SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment," IEEE Trans. Ind. Informatics, vol. 14, no. 6, pp. 2629–2640, 2018, doi: 10.1109/TII.2018.2789442.

[6 ]S. A. Butt, J. L.,Diaz-Martinez,T., Jamal, A. Ali, E. De-La-Hoz-Franco,.etal "IoT Smart Health Security Threats," Proc. - 2019 19th Int. Conf. Comput. Sci. Its Appl. ICCSA 2019, pp. 26–31, 2019, doi: 10.1109/ICCSA.2019.000-8.

[7] Amoon, M.,Altameem, T.,Altameem, A. "Internet of things sensor assisted security and quality analysis for health care data sets using artificial intelligence based heuristic health management system," Meas. J. Int. Meas. Confed., vol. 161, p. 107861, 2020, doi: 10.1016/j.measurement.2020.107861.

[8] Wu, C. T. Li, T. Y., C. L. Chen, C. C. Lee, and C. M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," Sensors (Switzerland), vol. 17, no. 7, 2017, doi: 10.3390/s17071482.

[9] Chen, Y.,W. Chen, "Finger ECG-based authentication for healthcare data security using artificial neural network," 2017 IEEE 19th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2017, vol. 2017-Decem, pp. 1–6, 2017, doi: 10.1109/HealthCom.2017.8210804.

[10] Williams, P. A. H.,McCauley, V. "Always connected: The security challenges of the healthcare Internet of Things," 2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016, pp. 30–35, 2017, doi: 10.1109/WF-IoT.2016.7845455.

[11] Mahmoud, R.,Yousuf T., F. Aloul,.I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015, pp. 336–341, 2016, doi: 10.1109/ICITST.2015.7412116.

[12] Huang, X. ,S. Nazir, "Evaluating Security of Internet of Medical Things Using the Analytic Network Process Method," Secur. Commun. Networks, vol. 2020, 2020, doi: 10.1155/2020/8829595.

[13] Lakkis, S. I.,Elshakankiri, M. "IoT based emergency and operational services in medical care systems," Jt. 13th CTTE 10th C. Conf. Internet Things - Bus. Model. Users, Networks, vol. 2018-Janua, pp. 1–5, 2017, doi: 10.1109/CTTE.2017.8260983.

[14] Thamilarasu, G.,Odesile, A.,Hoang, "An Intrusion Detection System for Internet of Medical Things," IEEE Access, vol. 8, pp. 181560–181576, 2020, doi: 10.1109/access.2020.3026260.

[15] Luo, E., Bhuiyan, M. Z. A. G., Wang, M. A.,et al "PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems," IEEE Commun. Mag., vol. 56, no. 2, pp. 163–168, 2018, doi: 10.1109/MCOM.2018.1700364.

[16] Farnaaz, N., Jabbar M. A., "Random Forest Modeling for Network Intrusion Detection System," Procedia Comput. Sci., vol. 89, pp. 213–217, 2016, doi: 10.1016/j.procs.2016.06.047.

[17] Kumar, R., Zhang, X., Wang,. Khan. W. R. U., "A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features," IEEE Access, vol. 7, pp. 64411–64430, 2019, doi: 10.1109/ACCESS.2019.2916886.