IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Review Article)

Check for updates

Security and privacy issues in IoMT

Dilruba Shareen [1, 2, *]

[1] *Department of Computer Science and Engineering, Khulna University of Engineering and Technology (KUET), Khulna, Bangladesh.*
[2] *Department of Statistics and Data Science, Jahangirnagar University, Savar, Dhaka-1342, Bangladesh.*

International Journal of Science and Research Archive, 2022, 07(02), 882-891

Publication history: Received on 18 November 2022; revised on 25 December 2022; accepted on 28 December 2022

Article DOI: https://doi.org/10.30574/ijsra.2022.7.2.0349

Abstract

The Internet of Medical Things (IoMTs) is gradually replacing the traditional healthcare system. However, little attention has been paid to their security requirements in the development of the IoMT devices and systems. One of the main reasons can be the difficulty of tuning conventional security solutions to the IoMT system. With this recent growing demand for IoMT, the associated technologies and its interconnected, heterogeneous nature add new concerns as it becomes accessible to confidential patient data, often without patient or medical staff consciousness, as the security and privacy of IoMT devices and technologies are often overlooked and undermined by relevant stakeholders. Hence, the growing security breaches that target the IoMT in healthcare are making the security and privacy of Medical IoT a crucial topic that is worth scrutinizing. In this study, we examined the current state of security and privacy of the IoMT, which has become of utmost concern among many security experts and researchers due to its rapid demand in recent times.

Keywords: Security; Privacy; IOT; Medical Internet of Things; Smart Health

1. Introduction

Technology integration is becoming an integral part of our daily life as a result of the technological advancement of various technologies [1]. This results in less manual work and aids in ubiquitously interconnecting everyone, and IoT plays a major role, offering smooth and seamless ubiquitous services for everyone [2,3]. In general, the IoT refers to the networking of physical devices that are smart and interconnected [4] and comprises sensors, software, and network connectivity that enables it to collect and exchange data [5,6]. Currently, the IoT is shaping and transforming both the business and consumer worlds, finding its way into every global business and consumer domain. Apart from this, it is also being delivered in many other domains, including healthcare, smart cities, agriculture, the military, and so on [4,5,6,7,8]. Hence, the IoT may significantly enhance the way people interact with the world. Based on recent reports, the IoT market size was valued at USD 761.4 billion in 2020 and is projected to reach USD 1386.06 billion by 2026, which signifies its importance as a dominant technological paradigm towards improving the well-being of billions of people all around the world [7,8].

When it comes to the IoT in healthcare, or what is well known as IoMT, it refers to a wide variety of IoT devices whose main purpose is to facilitate and aid in fundamental patient care [7,8]. the global IoT in healthcare market size is USD 71.84 billion in 2020 [9] and the market is projected to grow from USD 89.07 billion in 2021 to USD 446.52 billion by 2028 [9]. As of now, healthcare providers are utilizing various IoMT based applications and services for patient treatment, disease management, medical diagnosis, to improve patient care, and lower the costs of care, where they are capable of collecting various information such as vital body parameters from patients and monitor pathological details by implantable medical sensors or small wearable sensors that are worn by the patient. With the aid of IoMT devices, patient condition can be monitored remotely and in real-time, and the captured data can then be analyzed and

[*] Corresponding author: Dilruba Shareen

transmitted to the cloud data storage or the medical data centers for further processing and storage before offering services to various stakeholders such as physicians and other related medical staff, caregivers, and insurance service providers. In general, IoMT applications include solutions that are designed for remote health monitoring, emergency patient care, healthcare management, the monitoring of elderly patients, clinical decision support systems, wireless capsule endoscopy, and so on.

2. The Architecture of IoMT

As the main objective of this research study is to understand and review the current state of security and privacy aspects pertaining to the IoMT, it first is essential to understand the architecture and the devices and the technologies that are employed, as these creates a foundation towards better understanding the various security and privacy issues and their impact. We mainly discuss the architecture of the IoMT and the devices employed in each layer in the architecture.

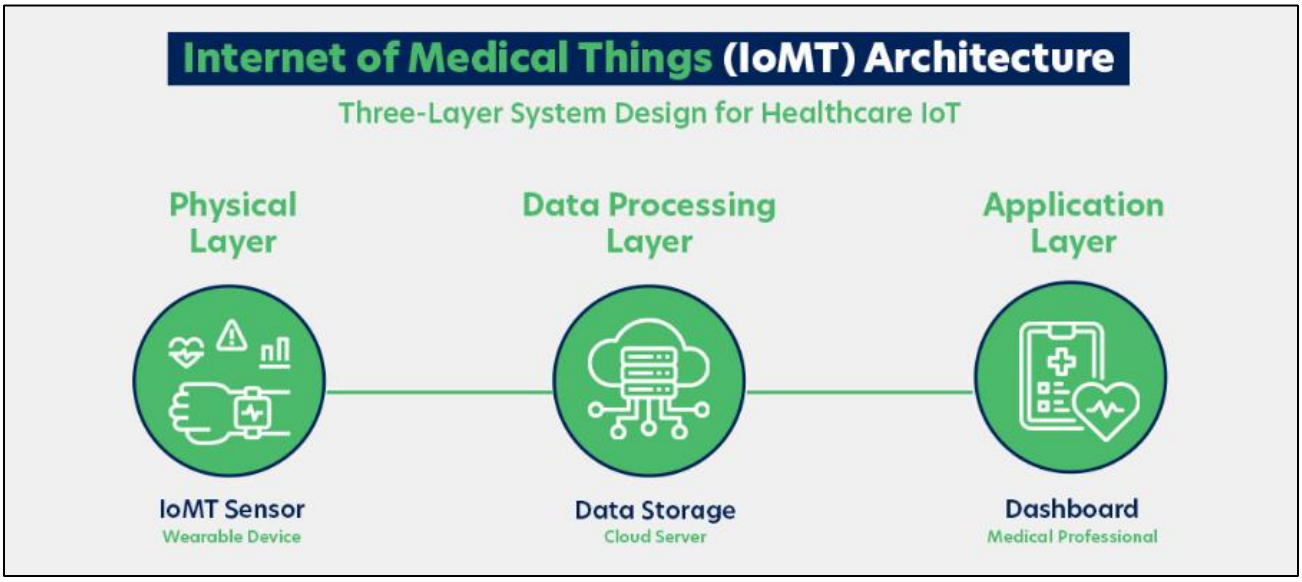


Figure 1 The three-layer architecture of the IoMT

- Physical/ Perception layer.
- Data Processing/ Network layer.
- Application layer.

According to the three-layered architecture, the bottommost layer is the perception layer, which is responsible for gathering the medical data from the physical IoMT devices, such as wearable's, smart blood glucose meters, ECG monitoring devices, and so on. Then, the network layer mainly consists of wireless, wired, and middleware systems, which facilitate the smooth delivery of gathered medical data, towards the destination. With the aid of underlying technological platforms, the network layer first processes and communicates the acquired data from the perception layer to the application layer, which is the topmost layer in the architecture. The application layer comprises medical data repositories to offer tailored and personalized medical services and to address the needs of end-users, who are patients, medical professionals, caregivers, and insurance companies. An important fact is that the underlying technologies used by each of these layers are different from one another. Altogether, the IoMT devices and integrated technologies are used to provide a variety of services, each with its own requirements and limitations.

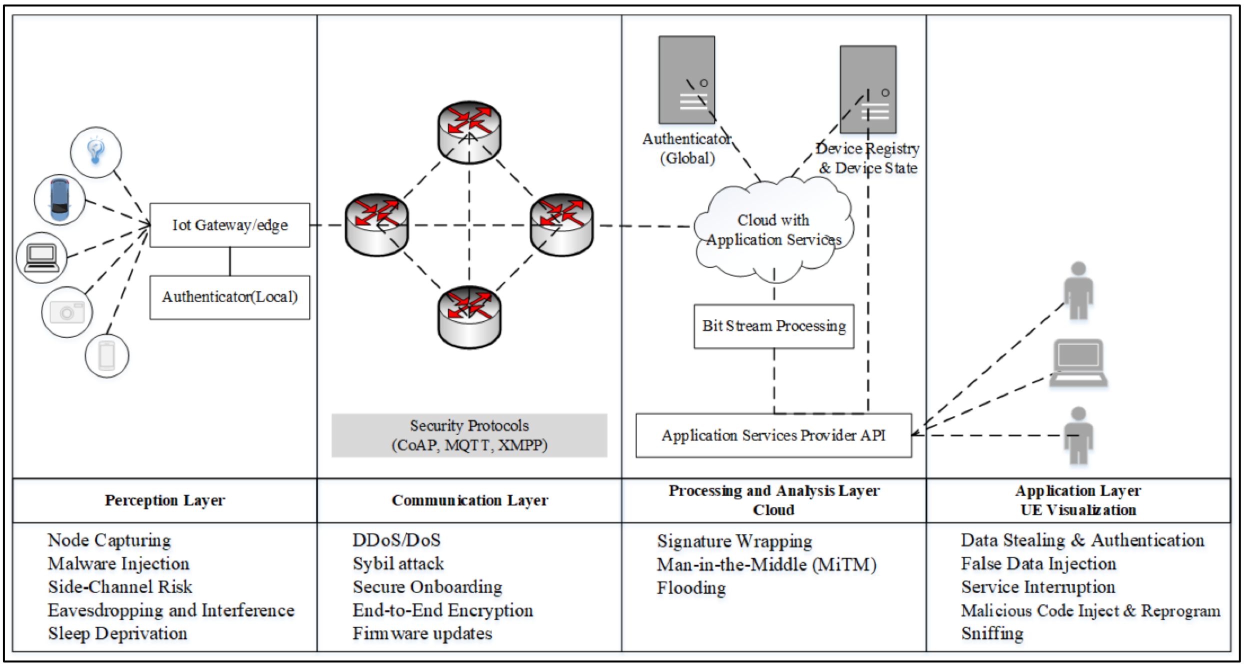
3. Sensor anomaly detection for medical devices

In [21], a sensor anomaly detection system was proposed to differentiate true from false alarms. The research used a historic data to be compared with the actual sensed data for prediction, whereas majority voting was used for their distinguishing. Consequently, the error was calculated based on dynamic threshold. The proposed method has been implemented in Java environment, supplied by the SMO regression. The results illustrated that the proposed system had a high Detection Rate and low FPR for three medical datasets. Furthermore, referring to the security of signals from deep brain stimulators, [22] built a system for distinguishing false alarms from legitimate ones and classified the attacks using Raspberry Pi3 and deep learning. It was found that deep learning can show an accuracy of about 97% to learn and predict the fake signals. Also, a web-based application was generated using the web engine (Flask) for that purpose.

Despite the effective application of ML algorithms, they are generating high computational overhead on the low-power embedded frameworks. [23] presented a neural network based MLP solution embedded on an FPGA chip system for securing insulin pump devices that are used by diabetic patients. The authors reported an accuracy of 98.1% for their system in distinguishing fake from genuine glucose measurements. The reliability of whole framework was improved by 18% in the case of securing one device and enhanced by 90% in the case of securing the whole devices. Khan et al. [24] proposed a personal server-centered (phone-based) Markov model-based detection mechanism for multiple intrusions such as forgery attacks, false data insertions, and data modifications in ECG data for smart medical devices. Analyzed results showed that the method has a high detection rate with abnormalities of 5% and 10% in the dataset and a higher TNR with reduced running time. In [25], some ML techniques were used, including decision tree, SVM and K-means, to detect the security attacks in implantable devices. An external detection device was used to monitor the network and the ML classifiers were utilized to detect anomalies on the gateway device for detecting forced device authentication that results in resource depletion of the device. For this purpose, a feature set specific to IMD devices was constructed. Experimental results demonstrated that decision tree-based algorithms achieved the highest detection accuracy, low false positive rate, fast training and prediction speed compared to those of other algorithms. In another study made in [26], SYNDROME was proposed. This method can detect code injection attack in a known program which runs on the system in a real time manner. Statistical based methods such as K–S test and external hardware device were used for detecting signal anomaly. The ability of the method was evaluated by implementing control-flow hijack attacks on a real medical device (syringe pump) embedded system. The evaluation results on using four distinct hardware systems have shown that the proposed model can detect all the attacks with 100% TPR and zero false positive, while the detection latency was less than 2 ms. In a pioneer work carried out by Zhang [27], a security framework was proposed for medical devices monitoring (MedMon). The proposed model was embedded on an external device which listens to all the passed signals coming from or sending to the medical devices by using a multi-layered anomaly detection (behavioral and physical anomalies). The system is useful for those medical devices that do not use encryption. Consequently, the framework either passively notifies the user or actively jams the signal. This solution does not add power overhead on the medical devices without modification to their software and hardware. An insulin delivery device was tested against the proposed method. Results depicted that the system could successfully detect multiple attacks. For the same purpose, a different approach has been proposed in [28] which is based on ML data-driven security framework, called HealthGuard, for detecting three types of malicious activities in a SHS by considering interconnected body function. Here, ML based techniques (Artificial Neural Network, Decision Tree, Random Forest, and k-Nearest Neighbor) were used to interpret the physiological signs in multiple attached SHS instruments and compare them to identify the differences in the person's body functions, thereby differentiating benevolent and malicious behaviors. Moreover, there is no need to have user identification for the medical devices, and the framework does not increase any overhead on the sensors while collecting data. The proposed system is trained with physiological data obtained from eight IoMT devices containing 12 genuine events consisting of 7 normal patient activities and five disease associated activities. Results showed an accuracy of 91% and F1 score of 90%. [29] suggested an anomaly data detection and separation for mobile smart healthcare. Two steps were implemented in the study, namely a preprocessing step and a real-time processing step. PCA and Correlation Coefficient were used for feature selection and feature extraction. By this, the system can detect false physiological readings and can distinguish between the false and true medical functions. [30] attempted to improve the detection efficiency by proposing an intrusion cancelation approach, thereby making the anomaly detection in medical devices efficient. This was achieved by using filters for eliminating noises in the medical data followed by detecting intrusions through statistically analyzed amplitude and frequency. Finally, the detected intrusions were removed to execute the anomaly detection in the medical device for diagnostic purpose. The simulation results applied on two sensor data showed that the system has high TPR and comparable FPR.

Table 1 Anomaly and attack detection to the sensors/medical devices

Ref.	Methods	Detection Type	Limitations	Tools	Dataset
[21]	SMO	Anomaly detection	high detection rate, low FPR	Weka	10 real datasets -(MIMIC)data
[22]	DL	Anomaly based false alarm detection	real time, high accuracy	Tensor flow and Keras in Python	John Radcliffe Hospital data
[23]	neural network based MLP	Anomaly based false alarm detection	real time, energy efficient, high accuracy, reliable	-NI myRIO -FPGA-based MLP	UCI Diabetic dataset
[24]	DWT and Marcov model	Anomaly based false data detection	high detection rate, high TNR, real time	MATLAB	The ECG dataset from MIT-PHYSIOBANK
[25]	Decision tree, SVM and K means	Anomaly-based attack detection	high accuracy, low FPR, low training time, low prediction time	Castalia	Simulation data
[26]	(K-S test) on external hardware device	malware Anomaly detection	high TPR, low FPR, low detection latency, no overhead on the medical device	-Open Syringe Pump -Arduino UNO, Nios-II, OlimexA13, and TS-7250	Testbed data
[27]	a model is embedded on an external device	multi-layered anomaly detection	zero overhead on battery, real time, multiple attacks detection, hybrid detection	USRP Glucose monitoring and insulin delivery systems	Testbed data
[28]	ANN, DT, RF, and k-NN	Anomaly detection using medical device data	high accuracy, high F1, No overhead on the sensors, uses body functioning data	MATLAB	A set of heath dataset from different sources
[29]	PCA and Correlation Coefficient	Anomaly based faulty sensor data detection	real time, lightweight, improved accuracy, improved FPR	-AUDITmodule -Java and R languages	MIMIC database
[30]	Statistical signal amplitude calculation	Anomaly based intrusion cancelation	using more than one type of Sensor type, high TPR	MATLAB	real medical ECG and EMG datasets



Perception Layer	Communication Layer	Processing and Analysis Layer Cloud	Application Layer UE Visualization
Node Capturing Malware Injection Side-Channel Risk Eavesdropping and Interference Sleep Deprivation	DDoS/DoS Sybil attack Secure Onboarding End-to-End Encryption Firmware updates	Signature Wrapping Man-in-the-Middle (MiTM) Flooding	Data Stealing & Authentication False Data Injection Service Interruption Malicious Code Inject & Reprogram Sniffing

Figure 2 Layered view of IoT for AA and Security Risks [50]

4. IOMT Authentication Schemes

IoT authentication security aims to identify and remove malicious nodes from the network [31]. The authentication process is a primary phase to validate the identity of the participating nodes in the IoT network. Even though only a few are considered to be ML-based, most studies in the literature emphasize detecting malicious nodes. Due to the scalability issue and the large number of things involved in exchanging sensitive data, intelligent AA security management is needed to enable multiple authorization factors to specific nodes.

Device-based authentication and authorization use client-side certificates stored on the machine. Verification occurs during the TLS handshake. As part of the handshake, the device sends its certificate, signed by a pre-configured signing authority. It sends the signed information with its private key. At the end of the handshake, the device is verified, and the client ID is removed from the certificate. For a machine, the customer ID may be the machine identification number (MIN) which is vital for verification from the server.

Once the machine has been verified, the customer ID is known. The next step is to determine the correct authorization groups. When connecting, a device can be part of a permission group. For example, a device is a machine, so all connecting machines are given the "machine" authorization group. It is possible to extract additional groups from the certificate and client ID. For example, it is possible to extract different groups of MIN from the machine. The mutual authentication of IoT systems is introduced in [32], which is established for client–server communication using the lightweight Application Layer Protocol CoAP (Constrained Application Protocol). Advanced encryption standard (AES) benefits are used as a secure communication channel. Authentication takes place on client and server challenges by encrypting the maximum payload size and interacting with the control loads. Authentication is performed during a messaging interaction without using an additional layer (DTLS), which increases communication and computing costs. The author also considered the robustness of the authentication scheme and dynamic registration of IoT nodes. Furthermore, average response time, handshake duration, and average memory consumption are discussed to benchmark the performance of the scheme. Additionally, the author showed attack tolerance to combat DoS-type attacks. The authors have not considered privacy and have not discussed the pre-shared key at the provisioning stage.

In [33], researchers proposed a lightweight multi-factor authentication strategy. The researchers utilized digital signature and device capacity for multi-factor authentication. The device capacity is similar to the resolved computational functionality of the device, which can be a mathematical problem-solving challenge or even a primitive puzzle based on cryptography. Moreover, authentication can utilize a strategy to authenticate both the end node and the server node. It can ensure security for both the application layer and physical layer. The end node sends a transmission request to the server through a protected TLS channel. The server node then transmits a private key and an encrypted timestamp message, which would prevent repetitive attack attempts. The end node decrypts the signature, addresses the ciphertext by functional procedure, registers the result with its personal key and returns them to the server node. The researchers also have explored MITM attacks and replay attacks tolerance. Eventually, the server node validates the signatures and the outcomes from the function during device authentication.

In [34], an Internet of Medical Things (IMT) authentication is proposed for devices that use human physical capabilities to communicate securely. Biometric techniques have been used for environments, while the analysis shows compatibility and safety, especially smart health. The authors presented the requirements for an intelligent health environment and discussed some of the open problems and challenges of biometric authentication.

A new authentication scheme for IoT systems has been proposed Bubbles-of-Trust by the authors of [35] which is based on blockchain. This mechanism aims to create bubbles by dividing devices into virtual zones to identify and trust each other through grouping. An Ethereum public blockchain is then applied to control and approve the transaction between devices. However, to validate a transaction, this consensus protocol takes a considerable amount of time, which is not feasible for real-time applications. Moreover, the transaction fee in the public blockchain is considered inefficient.

In [36], the lightweight two-factor authentication scheme is proposed to enable the authentication of Internet systems integrated with the one-way hashing and XOR-ing in the cloud computing environment. Registering, verifying, and updating the password are steps in the authentication process. Moreover, costs and computational efficiency are also considered and demonstrated in an environment where resources are minimal. However, the cost of communication and the computation cost at the cloud are also higher and have not considered the attacks, e.g., DoS and DDoS.

In [37], researchers proposed a rigorous assessment of WSN-supported IoT trust models focused on various elements, such as interoperability and resource optimization. The analysis found that neither of these models had (1) attempted to bring together data fusion trust (DFT), communication trust (CT), and data perception trust (DPT) and (2) met IoT security requirements. Therefore, it is essential to provide integrated trust protection to the platform. This model aims to evolve the resources as per IoT applications authentication requirements.

In [38], the researchers proposed a method to manage the firewall rule that takes all firewalls on the network route into account. As every network firewall is implemented, anomalies between rules of the various firewalls may arise. The authors of [39] discover and correct these erroneous configurations using a formal data structure method. The process also allows optimization of simple firewall rule sets by elimination rules which are no required anymore. Although the initial objectives are to detect the wrong internal firewall configurations, it did not focus on resolving incorrect configurations in a distributed environment during the analysis and verification of other network components security configurations. The researchers of [40] identified attack patterns and ML for IoT security techniques, including IoT user authentication, malware detection, role-based access control, and secure downloading. It addresses several challenges in implementing security techniques for real IoT systems using ML, such as partial observation of the states, computational overhead and communication overhead, and backup security solutions.

Although only 20% of access control methods currently use trust assessments, according to the researchers of [41], it is still a promising security mechanism because of its ability to calculate node dynamic trust value. The process helps the trust rating of each node to be measured gradually. Moreover, the authors of [42] proposed using ML as an intelligent trust assessment to mitigate an on-off attack during authentication that would threaten the node's trust value. Additionally, security protection should introduce apparent authentication vulnerability, such as compromised node attacks. The researchers claim in [43] that TBAC (trust-based access control) reliable access-control computing on IoT networks is still relatively recent but widely deployed in commercial applications. The authors of [44] also suggested a control scheme that supports multidimensional reliability properties utilizing trust and IoT reputations. The trust assessment is centralized just as in other work owing to the resource constraints of the devices.

In [45], the researchers used PKI benefits by using X.509 digital certificates To ensure secure authentication among devices within IoT systems. For device identification and device integrity, such a certificate can be used. But analysis of security and the requirements of scalability for PKI-based IoT systems are not considered. The authors of [46] implied a new easy authentication protocol that uses physically unclonable function (PUF)-based RFID tags, where the steps consist of tag recognition, validation, and updating. Mostly, the tag is recognized by the reader. Second, the reader and the label mutually verify authenticity. Finally, the most recently used password is updated for the next confirmation. However, the authors have not considered it in various environments.

Datagram Transport Layer Security (DTLS) protocol allows the client-server application to communicate securely over Transport Layer Security (TLS) protocol [47], while TLS deals with the information forging, altering, and fragmentation

[48]. DTLS deals with re-ordering packets, loss, and size of the datagram without considering Denial of Service (DoS) attacks.

In [49], the researchers proposed a hardware-driven authentication scheme for classical RFID tags for anonymous authentication of RFID systems. They then provided an improved scheme for a noisy physical unclonable function environment. The main disadvantage of this scheme is that it did not consider the challenge-response pair (CRP) server comments when an existing group is empty.

Table 2 Benefits and Limitations of Authentication schemes

Ref.	Benefit(s)	Limitation(s)
[31]	A centralized lightweight key-based Authentication scheme over CoAP. Able to detect DoS and eavesdropping attack.	Require more than four message exchange before establishing communication. Moreover, the end-to-end delay is not considered for benchmarking the performance, and it is not sufficient to tackle Sybil, MiTM, node capturing, and flooding attack.
[32]	A heterogeneous biometric authentication system that considered privacy profiling and tracking over the application layer.	Attacks are not considered, and performance metrics have not been properly considered for benchmarking. Moreover, the analysis of results is not adequately shown.
[33]	A lightweight two-factor authentication scheme using RFID tag with the one-way hashing and XOR-ing in the cloud computing environment. Moreover, costs and computational efficiency are also considered and demonstrated for the low-resource environment.	The cost of communication and the computation cost at the cloud are higher. Moreover, the attacks are not considered during authentication.
[34]	A lightweight, energy-efficient authentication scheme for a centralized IoT environment using X.509 PKI certificates is presented.	The practical analysis of security and scalability requirements for PKI-based IoT authentication systems are not considered. Moreover, attacks are not considered, and performance metrics have not considered properly for benchmarking.
[35]	A scalable, lightweight Authentication scheme with privacy profiling and tracking for IoT application layer is presented. A PUF key is shared as security credentials and provide tolerance against DoS and eavesdropping attacks. Moreover, the cost of communication and storage is minimal.	The end-to-end delay is not considered for benchmarking the performance, and it is not sufficient to tackle Sybil, MiTM, node capturing, and flooding attack.
[36]	A lightweight multi-factor authentication using digital signature and device capacity is presented. It can be utilized to authenticate both the end node and the server node from the application layer and physical layer perspective. Able to defence against MITM attacks and replay attacks.	The server node validates the signatures and the outcomes from the function during device authentication. At the same time, DoS/DDoS, Sybil attacks can take advantage, and considerable performance metrics are not discussed.
[37]	A blockchain-driven new authentication scheme for IoT systems aims to create bubbles by dividing devices into virtual zones to identify and trust each other through grouping.	To validate a transaction, this consensus protocol takes a considerable amount of time which is not feasible for real-time applications. Moreover, the transaction fee in the public blockchain is considered to be inefficient.

5. Conclusion

In this study, a comprehensive Systematic Literature Review (SLT) was given about the IoMT security and privacy issues and how Machine Learning (ML) methods are used for solving them. By examining the content of the study, including methods, good features, limitations, tools, and datasets, the designated research questions were answered. Findings of this study showed that ML techniques are effective in addressing the IoMT security issues with promising results.

Majority of the studies was devoted to device layer or body area network security since attacks on devices such as IMDs are seriously affecting the patient's health and life. The security solutions for such devices were sensor anomaly detection and device authentication and access control. Securing the network layer was seen among the studies that used attack and malware detection strategies.

References

[1] Subrato Bharati; M. Rubaiyat Hossain Mondal, "12 Applications and challenges of AI-driven IoHT for combating pandemics: a review," in Computational Intelligence for Managing Pandemics, De Gruyter, 2021, pp.213-230.

[2] Pinto Kumar Paul; Subrato Bharati; Prajoy Podder; M. Rubaiyat Hossain Mondal, "10 The role of IoMT during pandemics," in Computational Intelligence for Managing Pandemics, De Gruyter, 2021, pp.169-186.

[3] Hossain, M. B., Rahman, R., and Hoque, K. (2021). Feature-Driven Supervised Learning for Detecting DDoS Attack. International Journal of Science and Research Archive, 4(01), 393-402.

[4] Mahumd, T. (2022). ML-driven resource management in cloud computing. World Journal of Advanced Research and Reviews, 16(03), 1230-1238.

[5] Uddin, M. B., Hossain, M., and Das, S. (2022). Advancing manufacturing sustainability with industry 4.0 technologies. International Journal of Science and Research Archive, 6(01), 358-366.

[6] Hossain, M. B., and Rahman, R. (2022). Federated learning: Challenges and future work. World Journal of Advanced Research and Reviews, 15(02), 850-862.

[7] Tarouco, L.M.R.; Bertholdo, L.M.; Granville, L.Z.; Arbiza, L.M.R.; Carbone, F.; Marotta, M.; De Santanna, J.J.C. Internet of Things in healthcare: Interoperatibility and security issues. In Proceedings of the 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, USA; 2012; pp. 6121–6125.

[8] Hossain, M.; Islam, S.R.; Ali, F.; Kwak, K.S.; Hasan, R. An internet of things-based health prescription assistant and its security system design. Future Gener. Comput. Syst. 2018, 82, 422–439.

[9] Elhoseny, M.; Thilakarathne, N.N.; Alghamdi, M.I.; Mahendran, R.K.; Gardezi, A.A.; Weerasinghe, H.; Welhenge, A. Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions. Sustainability 2021, 13, 11645. https://doi.org/10.3390/su132111645.

[10] Grammatikis PIR, Sarigiannidis PG, Moscholios ID. 2019. Securing the internet of things: challenges, threats and solutions. Internet of Things 5(7):41–70 DOI 10.1016/j.iot.2018.11.003.

[11] Wazid M, Das AK, Rodrigues J, Shetty S, Park Y. 2019. IoMT malware detection approaches: analysis and research challenges. IEEE Access 7:182459–182476

[12] Fernandez Maimo L, Huertas Celdran A, Perales Gomez AL, Garcia Clemente FJ, Weimer J, Lee I. 2019. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors 19(5):1114 DOI 10.3390/s19051114

[13] Stiawan D, Idris M, Malik RF, Nurmaini S, Alsharif N, Budiarto R. 2019. Investigating brute force attack patterns in IoT network. Journal of Electrical and Computer Engineering 2019:1–13.

[14] 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

[15] Yaacoub J-PA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A. 2020. Securing internet of medical things systems: limitations, issues and recommendations. Future Generation Computer Systems 105(10):581–606 DOI 10.1016/j.future.2019.12.028

[16] Bharati, S., and Podder, P. (2022). Machine and deep learning for iot security and privacy: applications, challenges, and future directions. Security and communication networks, 2022(1), 8951961.

[17] Newaz AI, Sikder AK, Rahman MA, Uluagac AS. 2019. Healthguard: a machine learning-based security framework for smart healthcare systems. In: 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS). Piscataway: IEEE, 389–396.

[18] Alassaf N, Gutub A. 2019. Simulating light-weight-cryptography implementation for IoT healthcare data security applications. International Journal of E-Health and Medical Communications 10(4):1–15 DOI 10.4018/IJEHMC.2019100101.

[19] 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.

[20] Mosenia A, Jha NK. 2016. A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing 5(4):586–602 DOI 10.1109/TETC.2016.2606384.

[21] Haque SA, Rahman M, Aziz SM. 2015. Sensor anomaly detection in wireless sensor networks for healthcare. Sensors 15(4):8764-8786 DOI 10.3390/s150408764.

[22] Abdaoui A, Al-Ali A, Riahi A, Mohamed A, Du X, Guizani M. 2020. Secure medical treatment with deep learning on embedded board. Energy Efficiency of Medical Devices and Healthcare Applications 2020:131-151.

[23] Rathore H, Wenzel L, Al-Ali AK, Mohamed A, Du X, Guizani M. 2018c. Multi-layer perceptron model on chip for secure diabetic treatment. IEEE Access 6:44718-44730 DOI 10.1109/ACCESS.2018.2854822.

[24] Khan FA, Haldar NAH, Ali A, Iftikhar M, Zia TA, Zomaya AY. 2017. A continuous change detection mechanism to identify anomalies in ECG signals for WBAN-based healthcare environments. IEEE Access 5:13531-13544 DOI 10.1109/ACCESS.2017.2714258.

[25] Gao S, Thamilarasu G. 2017. Machine-learning classifiers for security in connected medical devices. In: 2017 26th International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE, 1-5.

[26] Sehatbakhsh N, Alam M, Nazari A, Zajic A, Prvulovic M. 2018. Syndrome: spectral analysis for anomaly detection on medical iot and embedded devices. In: 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). Piscataway: IEEE, 1-8.

[27] Zhang M, Raghunathan A, Jha NK. 2013. MedMon: securing medical devices through wireless monitoring and anomaly detection. IEEE Transactions on Biomedical Circuits and Systems 7(6):871-881 DOI 10.1109/TBCAS.2013.2245664.

[28] Newaz AI, Sikder AK, Rahman MA, Uluagac AS. 2019. Healthguard: a machine learning-based security framework for smart healthcare systems. In: 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS). Piscataway: IEEE, 389-396.

[29] Ben Amor L, Lahyani I, Jmaiel M. 2020. AUDIT: anomalous data detection and Isolation approach for mobile healThcare systems. Expert Systems 37(1):e12390 DOI 10.1111/exsy.12390.

[30] Mohamed MB, Meddeb-Makhlouf A, Fakhfakh A. 2019. Intrusion cancellation for anomaly detection in healthcare applications. In: 15th International Wireless Communications Mobile Computing Conference (IWCMC). Piscataway: IEEE, 313-318.

[31] Noor, M.B.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2018, 148, 283–294.

[32] Jan, M.A.; Khan, F.; Alam, M.; Usman, M. A payload-based mutual authentication scheme for Internet of Things. Future Gener. Comput. Syst. 2019, 92, 1028–1039.

[33] Alizai, Z.A.; Tareen, N.F.; Jadoon, I. Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures. In Proceedings of the 2018 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 4–5 September 2018; pp. 115–119.

[34] Hamidi, H. An approach to develop the smart health using Internet of Things and authentication based on biometric technology. Future Gener. Comput. Syst. 2019, 91, 434–449.

[35] Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Comput. Secur. 2018, 78, 126–142.

[36] Zhou, L.; Li, X.; Yeh, K.H.; Su, C.; Chiu, W. Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Gener. Comput. Syst. 2019, 91, 244–251.

[37] Souissi, I.; Ben Azzouna, N.; Ben Said, L. A multi-level study of information trust models in WSN-assisted IoT. Comput. Netw. 2019, 151, 12–30.

[38] Hu, H.; Ahn, G.J.; Kulkarni, K. Detecting and resolving firewall policy anomalies. IEEE Trans. Dependable Secur. Comput. 2012, 9, 318–331.

[39] Saâdaoui, A.; Ben Youssef Ben Souayeh, N.; Bouhoula, A. FARE: FDD-based firewall anomalies resolution tool. J. Comput. Sci. 2017, 23, 181–191.

[40] Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? IEEE Signal Process. Mag. 2018, 35, 41–49.

[41] Gong, B.; Zhang, Y.; Wang, Y. A remote attestation mechanism for the sensing layer nodes of the Internet of Things. Future Gener. Comput. Syst. 2018, 78, 867–886.

[42] Caminha, J.; Perkusich, A.; Perkusich, M. A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things. Secur. Commun. Netw. 2018, 2018, 6063456.

[43] Zhang, Y.; Wu, X. Access Control in Internet of Things: A Survey. In Proceedings of the Asia-Pacific Engineering and Technology Conference (APETC 2017), Kuala Lumpur, Malaysia, 25–26 May 2017; pp. 1544–1557. [Google Scholar]

[44] Bernal Bernabe, J.; Hernandez Ramos, J.L.; Skarmeta Gomez, A.F. TACIoT: Multidimensional trust-aware access control system for the Internet of Things. Soft Comput. 2016, 20, 1763–1779.

[45] Karthikeyan, S.; Patan, R.; Balamurugan, B. Enhancement of Security in the Internet of Things (IoT) by Using X.509 Authentication Mechanism. In Recent Trends in Communication, Computing, and Electronics; Springer: Singapore, 2019; pp. 217–225.

[46] Xu, H.; Ding, J.; Li, P.; Zhu, F.; Wang, R. A lightweight rfid mutual authentication protocol based on physical unclonable function. Sensors 2018, 18, 760.

[47] Modadugu, N.; Rescorla, E. The Design and Implementation of Datagram TLS. In Proceedings of the NDSS, San Diego, CA, USA, 5–6 February 2004.

[48] Raza, S.; Shafagh, H.; Hewage, K.; Hummen, R.; Voigt, T. Lithe: Lightweight secure CoAP for the internet of things. IEEE Sens. J. 2013, 13, 3711–3720.

[49] Gope, P.; Lee, J.; Quek, T.Q. Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions. IEEE Trans. Inf. Forensics Secur. 2018, 13, 2831–2843.

[50] Istiaque Ahmed, K.; Tahir, M.; Hadi Habaebi, M.; Lun Lau, S.; Ahad, A. Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction. Sensors 2021, 21, 5122. https://doi.org/10.3390/s21155122