STM JOURNALS

International Journal of
Wireless Security and Networks

ISSN: 2584-0703
Volume 3, Issue 2, 2025
July–December
DOI (Journal): 10.37591/IJWSN

https://journals.stmjournals.com/ijwsn

Review IJWSN

A Literature Review on Internet of Medical Things

Shalini Sachdeva[1,*], Rajesh Sachdeva[2]

Abstract

Artificial Intelligence (AI) is transforming healthcare by improving diagnostics, treatment planning, and patient management through data-driven insights and automation. The Internet of Medical Things (IoMT) represents a significant shift in modern healthcare, enabling real-time patient monitoring, data-driven decision-making, and enhanced medical outcomes. This literature review explores the architecture of IoMT, including perception layer, network layer, transport layer and application layer. It also thoroughly explores key challenges like ensuring data security, meeting regulatory requirements, and achieving seamless system interoperability. By analyzing recent studies and emerging trends, this review provides a comprehensive understanding of IoMT's role in transforming healthcare delivery. It examines key technologies, including wearable sensors, remote monitoring systems, and AI-driven analytics, while also addressing critical concerns such as cybersecurity, interoperability, and data privacy. Moreover, this study emphasizes recent research on how the Internet of Medical Things (IoMT) influences patient health outcomes, enhances healthcare efficiency, and contributes to lowering costs.

Keywords: Confidentiality, artificial intelligence, IoMT, integrity, security, wearable devices

INTRODUCTION

IoT (Internet of Things) networks are composed of connected physical devices, objects, and systems that share and transmit data via the internet or other communication channels. Commonly known as "smart" devices, they are equipped with sensors, software, and various technologies that allow them to gather and send information. IoT networks facilitate seamless data sharing, remote monitoring, and control of devices, enabling a wide range of applications across various domains [1]. These networks can include a diverse array of devices, such as wearable devices, home appliances, industrial machinery, vehicles, environmental sensors, and more, all working together to provide enhanced functionality, automation, and data-driven insights.

Analyzing this data provides valuable insights for businesses and organizations to make informed decisions, optimize operations, and develop new services. In the realm of smart homes, IoT networks allow for interconnected devices that can be controlled remotely [1–10]. IoT technology offers convenience in various areas, including home security, energy optimization, and entertainment systems. In the healthcare sector, it enables continuous patient monitoring, improving diagnosis, treatment, and chronic disease management. Environmental IoT sensors track factors like air quality, pollution, and water resources, supporting sustainable practices and conservation. In smart cities, IoT enhances urban living by streamlining traffic control, waste management, public safety, and utility services.

***Author for Correspondence**
Shalini Sachdeva
E-mail: Sachdeva.shalini86@yahoo.in

[1]Assistant Professor, Department of Computer Science and Applications, Ram Sukh Das College Ferozepur, Firozpur, Punjab, India
[2]Assistant Professor, Department of Computer Science, Dev Samaj College for Women, Firozpur, Punjab, India

Received Date: May 26, 2025
Accepted Date: August 05, 2025
Published Date: September 09, 2025

Citation: Shalini Sachdeva, Rajesh Sachdeva. A Literature Review on Internet of Medical Things. International Journal of Wireless Security and Networks. 2025; 3(2): 23–34p.

Within industrial settings, IoT helps anticipate equipment failures and maintenance needs through sensor data analysis, minimizing downtime and reducing expenses. In agriculture, IoT facilitates precision farming by observing soil conditions, crop health, and weather patterns, resulting in better resource efficiency and higher yields.

As of January 2023, the enterprise IoT market demonstrated a growth of 21.5%, reaching a value of $201 billion (Figure 1). This expansion was slightly below the previously projected 23% for the previous year and is anticipated to exhibit a further slowdown. Our earlier projection anticipated a more rapid global economic recovery, stronger supply chains, and sustained technological investments to counter labor shortages. The estimated spending growth for 2023 was initially predicted to be 24%; however, after revaluation, it has been revised down to 19%. Currently, IoT Analytics forecasts a Compound Annual Growth Rate (CAGR) of 19.4%, projecting the market to reach a value of $483 billion between 2022 and 2027. During this period, the Asia-Pacific (APAC) region is expected to outpace other global regions, boasting a CAGR of 22%. North America is projected to experience growth at a CAGR of 20%, surpassing Europe, which is estimated to grow at a CAGR of 16% until 2027.

IoT networks offer real-time tracking of goods, improving supply chain visibility, reducing delays, and minimizing losses. IoT drives innovation by opening the door to the development of new products and services. It also supports the emergence of novel business models, such as subscription-based offerings, data monetization, and other revenue-generating strategies. Devices connected to IoT networks can be remotely controlled, offering benefits in industries like energy management, asset tracking, and utilities. IoT networks enhance safety through applications like smart surveillance, emergency response systems, and wearable devices that monitor personal safety. In essence, IoT networks play a pivotal role in optimizing processes, generating insights, enhancing convenience, and driving innovation across a wide range of domains, ultimately leading to a more connected and efficient world [11–20].

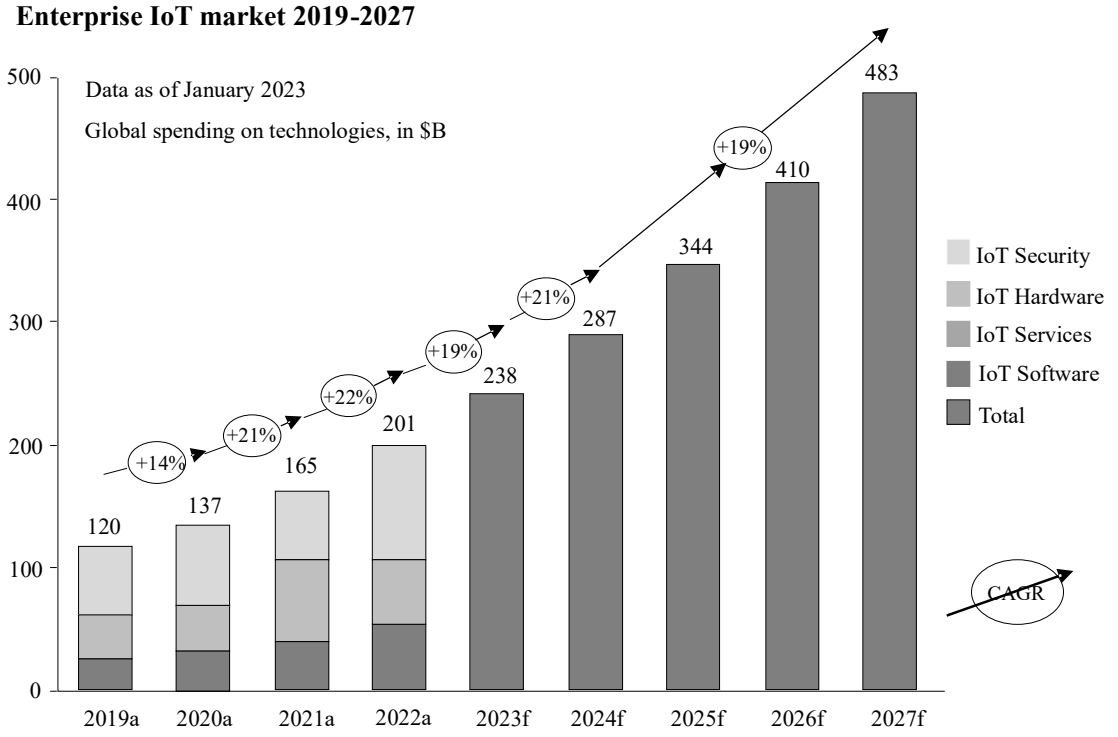

Figure 1. Global IoT market size to grow 19% in 2023 [6].

The integration of the Internet of Things (IoT) into healthcare has significantly enhanced patient care and the efficiency of medical operations. Recent advancements in IoT technologies have transformed the healthcare industry, driven by the rapid growth of internet-connected devices. According to Gartner, the number of IoT devices is expected to reach 27 billion by 2025, more than double the current count of smart devices. This transformation has introduced intelligent capabilities into medical equipment, giving rise to more advanced healthcare solutions. Today, healthcare monitoring systems are increasingly built with IoT due to the affordability and low power consumption of modern sensors. These sensors enable real-time remote monitoring of patients, reducing the constant need for doctors to be physically present.

The application of IoT in medical devices, commonly referred to as the Internet of Medical Things (IoMT), has gained substantial traction, now accounting for nearly 30% of the overall IoT device market. Progress in wireless communication and IoT has supported a wide variety of healthcare applications, including patient monitoring, early disease detection, remote treatment, and emergency response systems.

Implementing reliable and secure methods for critical medical emergencies can reduce reliance on physicians and lower healthcare costs. Intelligent decision-making systems also contribute to earlier interventions, potentially saving lives. Wearable health monitoring devices play a key role in continuously assessing the health status of individuals within connected communities. This allows healthcare providers to deliver timely diagnostic and monitoring services in smart environments.

However, security is a major concern. If compromised, these systems can lead to serious breaches of sensitive patient data and privacy, and in severe cases, may even result in patient fatalities. According to a report by Cynerio, many IoT-enabled medical devices are vulnerable to critical security flaws. Unauthorized exposure of these devices increases the risk of cyberattacks, potentially allowing hackers to access patient records. Attackers may exploit known vulnerabilities and employ Advanced Persistent Threats (APTs) to take control of targeted devices, posing serious risks to patient safety.

As such, securing IoMT-based healthcare systems must be a top priority. Various strategies can be adopted to detect and prevent cyber threats. Common types of attacks on IoMT networks include Denial of Service (DoS), injection of malicious traffic, and Man-in-the-Middle (MITM) attacks, all of which aim to disrupt or compromise system functionality.

Various techniques like are used for detection and mitigation purposes:

- Intrusion Detection Systems (IDS),
- Vulnerability management,
- Log monitoring,
- End device monitoring,
- Prevention systems, and
- Threat intelligence.

Among these systems, IDS is a modern technology used to recognize various network attacks and security issues in IoMT [1, 3].

RELATED WORK

Many researchers have proposed several methods for designing smart health monitoring systems. Fotouhi *et al.* developed a healthcare monitoring framework comprising three components, i.e., a gateway, an Access Points (APS), and a coordinator [1]. The coordinator is defined as the node that is attached to the body of the patients for gathering information related to patient's health using sensors. In the room's walls, static nodes, also called access points, are located by the sensors that use communication protocols (like 6LoWPAN, BLE, or ZigBee). The information gathered by the APs gets

forwarded to the gateway. Then using the internet, this information gets transferred to the cloud server. Without proper testing and explanation, some techniques have been proposed in this system for securing the data. Clifton *et al*. explained the ML technique's role in health monitoring systems [9]. These techniques have been used for controlling and managing false alerts while revealing serious health issues. The data used in their experiment is a combination of the patient's clinical observations to provide quick alerts in an envisaged emergency. This work has been conducted at Oxford University Hospital [21–30].

Rani *et al*. introduced a cloud-based healthcare platform that uses an SVM (Support Vector Machine) approach to forecast patients' situations and envisioned diseases [10]. No unauthorized users are permitted in the system. Blockchain-based healthcare system framework has been designed by Chakraborty *et al*., which is helpful in overcoming the problems associated with the traditional healthcare system related to the security issues of the records created during the treatment of the patient [11]. The framework has been set up for supervising the treatment process all over the time from beginning to end. Alabdulatif *et al*. developed a cloud-based smart prediction framework [12]. This system was based on Fully Homomorphic Encryption (FHE) approach. This system comprises three blocks, i.e., the smart community resident, cloud storage, and smart prediction model. In the first block, the data is gathered and dispatched to the cloud storage repository system. The encrypted data gets amassed in the second block. The third block has been used to detect anomalous changes like attacks without decrypting data. A secured anticipating approach based on Holt's linear trend method has been developed that is used to predict anomalous changes in the vital sign of patients, which helps to detect different chronic diseases. The author also introduced a novel parallel technique of Holt's method for improving the effectiveness of the FHE model.

Tao *et al*. introduced a Secure Data scheme that delivers both privacy and security to the patient's private records [13]. FPGA (Field Programmable Gate Array) platform is used for the optimization of the KATAN secret algorithm, which is implemented for secure communication.

A security system has been suggested by Zhang *et al*. that applied RF (Random Forest) technique to detect anomaly traffic on KDD 1999 dataset [14]. With a 1% false positive rate, this technique achieves 95% accuracy as an anomaly detector. This dataset is employed to test anomaly detection algorithms. It is a generic Knowledge discovery and data mining dataset. Since 1999, this dataset has been used in many competitions. Rao *et al*. employed the Indexed Partial Distance Search k-Nearest Neighbor (IPDS-KNN) technique that is employed to assess a diverse variety of attacks [15]. It achieved 99.6% of accuracy performance. Shapoorifard *et al*. use the k-Nearest Neighbor (KNN) technique, which achieves 85.2% of accuracy [16]. The author mainly emphasizes on decreasing the False Alarm Rate (FAR). To forecast various attack simulations in Deep Brain Stimulators (DBSs), Rathore *et al*. [17] developed a DL algorithm that efficiently identifies the pattern of attacks and alerts a patient [31–40].

To overcome the attack detection problem in IoMT, Yaacoub *et al*. discussed different types of ML-based privacy and security solutions [18]. But, according to the author, there is still a need to introduce an effective IDS system to detect attacks. To analyze attacks in the smart hospital, an ensemble classifier IDS has been developed by Saba [19]. The Decision Tree (DT) technique attained 93.2% of accuracy performance in categorizing the cyber-attacks in the KDDcup-99 dataset. This dataset was created in the traditional network without adding IoT device traffic. Kumar *et al*. performed the experiment in three stages. In the first stage, the author introduced an ensemble of the RF, naïve Bayes (NB), and DT [20]. In the second stage, to categorize both regular and attack network records, XGBoost was applied. In the third stage, to categorize the attacks in the IoMT environment, the developed model was then applied to the ToN-IoT dataset, which attained 96.35% of the accuracy. The industrial IoT network setup has been used to create this dataset using Modbus weather sensors. In the IoMT environment, these sensors are not commonly employed. Therefore, the data presented above could not be appropriate for identifying network attacks.

Radoglou *et al*. developed an Intrusion detection and prevention system (IDPS) for the identification and prevention of various cyberattacks against communication protocols like Modbus/TCP and HTTP, which are broadly used by e-healthcare services [21]. EHR uses HTTP, whereas IoMT uses Modbus/TCP protocol. The proposed IDPS can retrain ML techniques and test itself using an active learning approach. The CIC-IDS2017 dataset was employed in this experiment to analyze the functioning of ML techniques on the HTTP network dataset. DT classifier achieved an accuracy of 96.44% in categorizing network attacks. In comparison, RF attained 94.45% of the accuracy on the Modbus dataset.

Zachos *et al*. introduced a systematic and potent Anomaly-based IDS (AIDS) for the IoMT environment [22]. To devise a unique feature set, the three features, i.e., gateways, IoT device features, and network traffic features, were combined together. To enhance the functionality of attack detection, various ML techniques have been applied to identify deviations in the gathered malicious and data events in the network. For evaluation in IoT devices, memory consumption level attributes, and CPU were taken into consideration. The TON_IoT Telemetry dataset has been used in this experiment. According to the result reported by the author, KNN, RF, and DT are the most appropriate ML techniques that are employed for the central detection integrant of the introduced system.

A mobile agent-based IDS has been introduced by Thamilarasu *et al*. to identify both network and device-based attacks in the IoMT environment [23]. The simulation-generated datasets were tested using ML and regression techniques. Using the DT technique in the evaluation process, the device and network-level intrusion detection achieve an accuracy of 97.93 and 99.8%, respectively.

Binbusayyis *et al*. inspected and showed a detailed comparison of different techniques like KNN, SVM, ANN (Artificial Neural Network), NB, and DT [24]. The Bot-IoT dataset was used in the experiment to compare the working performance of ML methods. This dataset comprises various attack categories like Denial of service (DoS), theft attacks, and Distributed Denial of Service (DDoS) attacks. Spoofing attacks and MITM attacks are IoMT attacks that are not covered in this dataset. On the tested dataset, DT attained an accuracy of 100%, and other ML techniques like SVM, NB, and KNN achieved an accuracy of 99%.

As per the study, ML techniques are used to identify attacks in IoMT. But most of the datasets were created without considering the IoMT environment and attacks. The result presented by the authors in their research were outstanding, as in many contributions, the ML techniques achieved an accuracy of 95%. For the IoMT study, many input features like IoT device memory, network traffic, CPU features, or metric features were considered. But features like patient biometric data were not used or mentioned by any researchers in their work to identify cyber-attacks in the IoMT. To classify or identify the attack in the IoMTeco system, many researchers explored DL techniques [41–50].

For feature selection, Saheed *et al*. used Particle swarm optimization (PSO) and applied ML/DL-based techniques to identify cyber-attacks in the network. Researchers used the NSL-KDD dataset to analyze the functionality of the suggested technique [25]. The introduced model attained 99.76% of the accuracy performance. This dataset was not created by keeping the IoT environment in mind and should not be used to assess attack identification in IoMT.

Awotunde *et al.* developed a swarm neural network (SNN)-based method that detects intruders while transmitting the data and permits accurate and efficient assessment of medical data at the network edge [26]. For the experiment, the author used NF-ToN-IoT dataset, which is the amalgamation of network data, operating systems, and telemetry. The researcher employed a deep autoencoder (DAE) to reduce the dimensionality of the feature set. To recognize the network attacks, the author used a deep feed-forward neural network (DFFNN) in the IoT environment. The DAE-DFFNN model achieved an accuracy of 89%, which is superior to ML techniques such as DT and SVM as claimed by the researcher.

For identifying malware in the IoMT ecosystem, Khan *et al*. introduced SDN (Software Defined Network) enabled CNN (Convolutional Neural Network) and LSTM (Long short-term memory) hybrid DL model, which attained an accuracy of 99% [27]. Howbeit, this framework was not used as IDS to determine network attacks in IoMT ecosystem. Nandy *et al*. developed intelligent agent-based SNN for detecting intruders in IoMT [28]. The experiment was conducted using the proposed approach on the ToN-IoT dataset, which attained 99.5% of the accuracy. To identify the network attack in the IoT environment, Manimurugan *et al*. introduced a DL-based deep belief network (DBN) algorithm that achieved an accuracy of 96% [29]. The experiment was conducted using the proposed model on the CICIDS dataset. This dataset generation did not concentrate on IoMT network attacks.

The above study of DL approaches indicates that these techniques were not highly introduced to identify IoMT network attacks. Most of the authors only explored the network traffic dataset in their experimental work to identify the attacks in the network.

IoMT ARCHITECTURE

Many architectures were presented in the literature. Some researches proposed architectures composed of three layers [16, 17]. Other researches proposed using an architecture with more than three layers [18]. Various technologies have been suggested for handling medical data, including fog and cloud computing [19], Software-Defined Networking (SDN) [20], and Blockchain [21]. This review work proposes a three-tier architecture as an effective approach to logically structure the IoMT system. The three layers: data acquisition, personal server, and medical server, are described in detail below and depicted in Figure 2.

Data Acquisition Layer

Sensor devices act as a connection between the human body and the digital environment. They can be categorized into four types [17, 18]:

1. *Implanted devices:* these are positioned within the human body, such as Deep Brain Implants (DBIs).
2. *The wearable devices:* these devices are on the human body e.g., Smartwatch, Pulse Generator (PG), or Electroencephalogram (EEG).
3. *The ambient devices:* these devices allow capturing data from the environment around the patient, e.g., room temperature sensors.
4. *The stationary devices:* these sensors are located in the hospital, e.g., imaging devices.

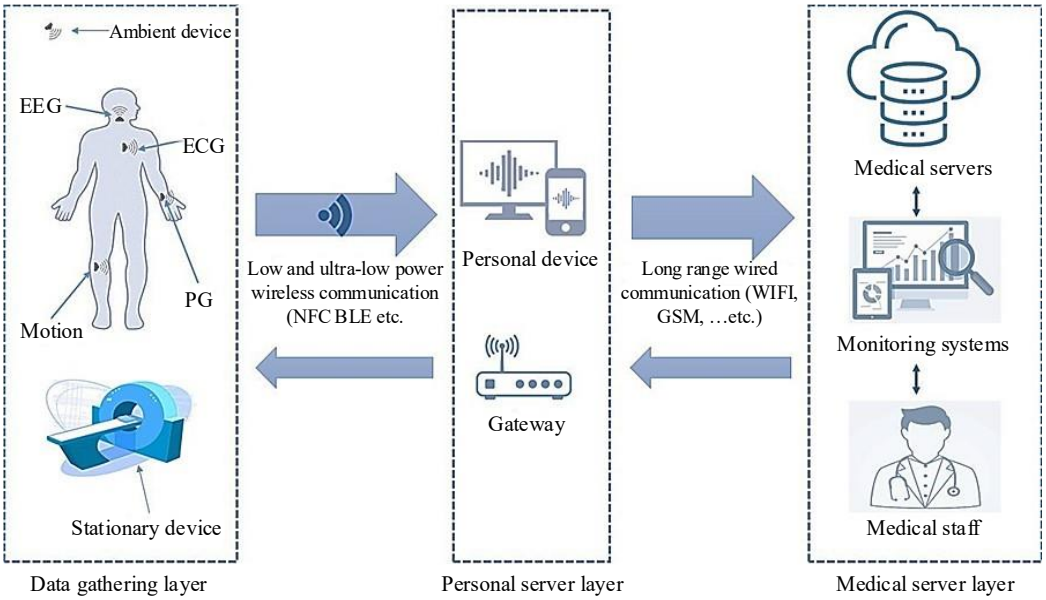

Figure 2. Internet-of-Medical-Things(IoMT) Architecture.

These devices come equipped with physiological sensors as well as low-power computing, connectivity, and storage components, which enable them to collect biomedical and contextual signals [22]. The gathered data are utilized to support patient diagnosis and treatment management. However, these medical devices face several limitations both internally and in terms of communication. Internally, implants within the body may be rejected by the patient's immune system, causing inflammation and discomfort. Additionally, the battery life of these devices is limited and requires replacement after several years. Conventional security techniques like cryptography can drain the battery faster, necessitating risky surgical procedures for replacement. Due to limited memory capacity, these devices cannot maintain logs of their data exchanges. In terms of communication, the devices are restricted to short-range transmissions because of energy constraints [9]. Most wearable devices have limited processing power and therefore only perform initial data processing. The embedded low-power computing modules compress the collected data before transmitting it to personal devices such as smartphones or computers via low-energy wireless technologies like Near Field Communication (NFC) or Bluetooth Low Energy (BLE) [23].

Personal Server Layer

Medical devices transmit physiological data to personal servers such as smartphones, laptops, or gateway devices [24]. These personal servers handle the processing and temporary storage of patient data before forwarding it to centralized medical servers. Upon receipt, the data may be enriched with contextual details like location and time to identify abnormal behavior. The data can also be encrypted or compressed before being sent to remote medical servers in standardized formats like Health Level-7, using long-range wireless protocols such as Wi-Fi, GSM, or wired connections [10]. This layer supports diverse communication methods and device mobility and ensures data can be retransmitted if the network connection to medical servers is interrupted [11, 25].

Medical Server Layer

This layer comprises a high-capacity data center designed for centralized patient monitoring, advanced and long-term behavior analysis, and integration of patient data from multiple sources. It also includes a cloud server that makes intelligent decisions. It is used for data aggregation and provides extra patient medical data storage. The doctors, patients, and the pharmacy department (for summary or billing purposes) can access these data. Patients may use an online interface or smartphone to display their past and current health records/bills. Data from various sources are incorporated into EHR, Electronic Medical Records (EMR), or prescription websites. Consequently, both doctors and patients have access to the information whenever required. It also offers a notification system to alert patients whenever health data is uploaded or received [26].

SECURITY REQUIREMENTS OF IoMT

The Internet of Medical Things (IoMT) relies on wireless communication and the internet to send data gathered from the human body to medical servers. As a result, the data across the various layers of the IoMT system, depicted in Figure 2, are vulnerable to cyberattacks that can compromise patient privacy and potentially threaten their lives. To protect against these threats, it is essential to fulfill security requirements that enable prevention, detection, and real-time response to such attacks. This section outlines the key security needs of IoMT, as shown in Figure 3 [51–55].

Confidentiality

This requirement guarantees that patient health information and identifying details remain inaccessible to unauthorized individuals during both data storage and transmission. Protecting confidentiality prevents sensitive information from being exposed to malicious parties who could potentially harm the patient [11, 27].

Integrity

Ensuring data integrity in IoMT healthcare systems means that information reaching its intended recipient remains unaltered during wireless transmission.

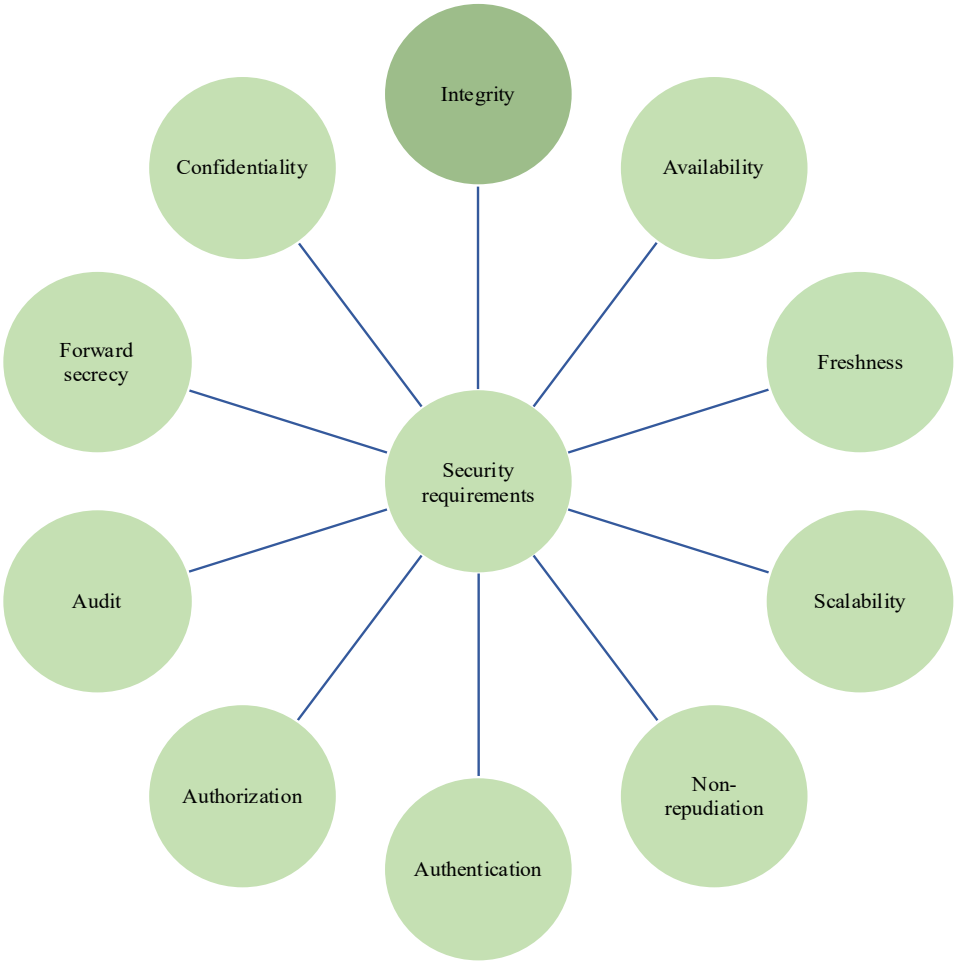

Figure 3. Security requirements in IoMT.

Even minor modifications to medication details or test results could have serious consequences for patient safety. Maintaining integrity prevents unauthorized alterations by anyone other than authorized personnel, such as doctors or nurses, thereby avoiding incorrect treatments [24].

Availability

Healthcare and clinical records must be continuously accessible to doctors at any time and location without interruption. Prompt response to emergencies is critical for providing timely treatment or precautionary measures. One approach to maintain availability is to reroute from compromised nodes to alternative nodes within the network, a capability supported by network and system design [24, 25].

Freshness

This requirement ensures that health data is current and guards against the reuse of outdated medical information by attackers. Freshness can be classified as weak or strong: weak freshness provides partial ordering of messages without delay details, whereas strong freshness offers complete ordering and allows delay measurement [10, 28].

Scalability

Scalability refers to the IoMT network's ability to operate efficiently as the number of connected devices grows. Poor scalability can introduce security vulnerabilities, making it crucial to manage computing and storage overhead effectively, especially during emergencies where rapid response is essential [29, 30].

Non-repudiation

Non-repudiation ensures that no party involved in the healthcare process can deny having sent or received patient health information, maintaining accountability within the system [13].

Authentication

In healthcare systems, authentication applies to both data and individuals. Data authentication verifies the original source of the information to ensure its legitimacy. Person authentication in communications between patients and related servers should be checked through accurate identity authentication. Therefore, before they communicate or exchange any details, all parties need to know each other. Before any data sharing occurs, the healthcare system must identify each participant to confirm that the user is authorized to access the stored information. It is crucial to determine the user's privilege level to establish what type of data they are permitted to view or use [12, 24].

Authorization

Authorization controls define the access rights of users, whether patients, doctors, or nurses, regarding the medical database. The healthcare provider is responsible for approving users and specifying the extent of data access each individual is allowed [13, 27].

Audit

Auditing involves reviewing system modifications and monitoring access to patient medical records by examining log files, which maintain historical information about hardware and software activity. This process helps identify unusual behavior and potential security breaches. However, managing and analyzing these logs can be challenging due to their volume and diversity, stemming from various medical and network devices.

Forward Secrecy

Backward secrecy ensures that medical sensors joining the network at a later time are unable to decrypt messages sent prior to their inclusion in the network [30].

- *Forward secrecy:* Medical sensors that have left the network are unable to read messages received after their exit [30].

CONCLUSION

The deployment of ML models in medical equipment presents a challenge due to its various limitations. Three deployment approaches have been suggested: embedding the machine learning (ML) model directly into medical devices, deploying it on an external third-party device, or integrating the model onto a chip that is then incorporated into the medical equipment. One major obstacle for researchers is the scarcity of publicly available datasets specifically created for security purposes that also include medical data. This limitation complicates the development of intrusion detection systems (IDS) that must support a wide variety of connected medical devices, each with its own unique data collection and communication protocols. Using an imbalanced dataset to train ML models introduces issues such as biased outcomes, overfitting, and challenges in accurately assessing performance with standard evaluation metrics. Therefore, careful handling of the dataset's imbalance is crucial during model development. Additionally, the data format and structure used to train ML models on medical servers differ from those on other servers, which makes it difficult to generalize the model for use across different healthcare institutions.

REFERENCES

1. Fotouhi H, Causevic A, Lundqvist K, Bjorkman M. Communication and security in Health Monitoring Systems -- a review. 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). 2016; 545–554. https://doi.org/10.1109/compsac.2016.8
2. Satyajit Sinha. (2024 Sep 3). State of IOT 2022: Number of connected IOT devices growing 18% to 14.4 billion globally. [Online]. IoT Analytics. Retrieved February 20, 2023, from https://iot-analytics.com/number-connected-iot-devices/

3. Cogniteq. (2022 Jan 20). Internet of medical things (IOMT): Innovative Future for Healthcare Industry. [Online]. Cogniteq. Retrieved February 20, 2023, from http://www.cogniteq.com/blog/internet-medical-things-iomt-innovative-future-healthcare-industry
4. Newman LH. (2022 Mar 8). Critical bugs expose hundreds of thousands of medical devices and atms. [Online]. Wired. Retrieved February 20, 2023, from https://www.wired.com/story/access7-iot- vulnerabilities-medical-devices-atms/
5. Ravi V, Alazab M, Selvaganapathy S, Chaganti R. A multi-view attention-based deep learning framework for malware detection in Smart Healthcare Systems. Comput Commun. 2022; 195: 73–81. https://doi.org/10.1016/j.comcom.2022.08.015
6. Radoglou-Grammatikis P, Sarigiannidis P, Efstathopoulos G, Lagkas T, Fragulis G, Sarigiannidis A. A self-learning approach for detecting intrusions in Healthcare Systems. ICC 2021 - IEEE International Conference on Communications. 2021; 1–6. https://doi.org/10.1109/icc42927.2021.9500354
7. Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R. Recent advances in the internet-of-medical-things (IOMT) systems security. IEEE Internet Things J. 2021; 8(11): 8707–8718. https://doi.org/10.1109/jiot.2020.3045653.
8. Hady AA, Ghubaish A, Salman T, Unal D, Jain R. Intrusion detection system for healthcare systems using medical and network data: A comparison study. IEEE Access. 2020; 8: 106576–106584. https://doi.org/10.1109/access.2020.3000421
9. Clifton L, Clifton DA, Pimentel MA, Watkinson PJ, Tarassenko L. Predictive monitoring of mobile patients by combining clinical observations with data from wearable sensors. IEEE J Biomed Health Inform. 2014; 18(3): 722–730. https://doi.org/10.1109/jbhi.2013.2293059
10. Rani AA, Baburaj E. Secure and intelligent architecture for cloud-based healthcare applications in Wireless Body Sensor Networks. Int J Biomed Eng Technol. 2019; 29(2): 186–199. https://doi.org/10.1504/ijbet.2019.097305
11. Chakraborty S, Aich S, Kim H-C. A secure healthcare system design framework using Blockchain technology. 2019 21st International Conference on Advanced Communication Technology (ICACT). 2019; 260–264. https://doi.org/10.23919/icact.2019.8701983
12. Alabdulatif A, Khalil I, Forkan AR, Atiquzzaman M. Real-time secure health surveillance for Smarter Health Communities. IEEE Commun Mag. 2019; 57(1): 122–129. https://doi.org/10.1109/mcom.2017.1700547
13. Tao H, Bhuiyan MZ, Abdalla AN, Hassan MM, Zain JM, Hayajneh T. Secured data collection with hardware-based ciphers for IOT-based healthcare. IEEE Internet Things J. 2019; 6(1): 410–420. https://doi.org/10.1109/jiot.2018.2854714
14. Jiong Zhang, Zulkernine M, Haque A. Random-forests-based network intrusion detection systems. IEEE Trans Syst Man Cybern Part C (Appl Rev). 2008; 38(5): 649–659. https://doi.org/10.1109/tsmcc.2008.923876
15. Rao BB, Swathi K. Fast knn classifiers for network Intrusion Detection System. Indian J Sci Technol. 2017; 10(14): 1–10. https://doi.org/10.17485/ijst/2017/v10i14/93690
16. Shapoorifard H, Shamsinejad P. Intrusion detection using a novel hybrid method incorporating an improved KNN. Int J Comput Appl. 2017; 173(1): 5–9. https://doi.org/10.5120/ijca2017914340
17. Rathore H, Al-Ali AK, Mohamed A, Du X, Guizani M. A novel deep learning strategy for classifying different attack patterns for deep brain implants. IEEE Access. 2019; 7: 24154–24164. https://doi.org/10.1109/access.2019.2899558
18. Yaacoub J-PA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A. Securing internet of medical things systems: Limitations, issues and recommendations. Future Gener Comput Syst. 2020; 105: 581–606. https://doi.org/10.1016/j.future.2019.12.028
19. Saba T. Intrusion detection in Smart City Hospitals using ensemble classifiers. 2020 13th International Conference on Developments in ESystems Engineering (DeSE). 2020; 418–422. https://doi.org/10.1109/dese51703.2020.9450247
20. Kumar P, Gupta GP, Tripathi R. An ensemble learning and fog-cloud architecture- driven cyber-attack detection framework for IOMT networks. Comput Commun. 2021; 166: 110–124. https://doi.org/10.1016/j.comcom.2020.12.003

21. Radoglou-Grammatikis P, Sarigiannidis P, Efstathopoulos G, Lagkas T, Fragulis G, Sarigiannidis A. A self-learning approach for detecting intrusions in Healthcare Systems. ICC 2021 - IEEE International Conference on Communications. 2021; 1–6. https://doi.org/10.1109/icc42927.2021.9500354
22. Zachos G, Essop I, Mantas G, Porfyrakis K, Ribeiro JC, Rodriguez J. An anomaly- based intrusion detection system for internet of medical things networks. Electronics. 2021; 10(21): 2562. https://doi.org/10.3390/electronics10212562
23. Thamilarasu G, Odesile A, Hoang A. An intrusion detection system for internet of medical things. IEEE Access. 2020; 8: 181560–181576. https://doi.org/10.1109/access.2020.3026260
24. Binbusayyis A, Alaskar H, Vaiyapuri T, Dinesh M. An investigation and comparison of machine learning approaches for intrusion detection in IOMT Network. J Supercomput. 2022; 78(15): 17403–17422. https://doi.org/10.1007/s11227-022-04568-3
25. Saheed YK, Arowolo MO. Efficient cyber attack detection on the Internet of Medical Things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access. 2021; 9: 161546–161554. https://doi.org/10.1109/access.2021.3128837
26. Awotunde JB, Abiodun KM, Adeniyi EA, Folorunso SO, Jimoh RG. A deep learning-based intrusion detection technique for a secured IOMT system. Informatics and Intelligent Applications. Cham: Springer; 2022; 50–62. https://doi.org/10.1007/978-3-030-95630-1_4 .
27. Khan S, Akhunzada A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for internet of medical things (IOMT). Comput Commun. 2021; 170: 209–216. https://doi.org/10.1016/j.comcom.2021.01.013
28. Nandy S, Adhikari M, Khan MA, Menon VG, Verma S. An intrusion detection mechanism for secured IOMT framework based on Swarm-Neural Network. IEEE J Biomed Health Inform. 2022; 26(5): 1969–1976. https://doi.org/10.1109/jbhi.2021.3101686
29. Manimurugan S, Al-Mutairi S, Aborokbah MM, Chilamkurti N, Ganesan S, Patan R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access. 2020; 8: 77396–77404. https://doi.org/10.1109/access.2020.2986013
30. Su J, DaniloVasconcellos V, Prasad S, Daniele S, Feng Y, Sakurai K. Lightweight Classification of IOT malware based on image recognition. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). 2018; 664–669. https://doi.org/10.1109/compsac.2018.10315
31. Nguyen H-T, Ngo Q-D, Le V-H. IOT botnet detection approach based on psi graph and DGCNN classifier. 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP). 2018; 118–122. https://doi.org/10.1109/icicsp.2018.8549713
32. Hussain F, Abbas SG, Fayyaz UU, Shah GA, Toqeer A, Ali A. Towards a universal features set for IOT botnet attacks detection. 2020 IEEE 23rd International Multitopic Conference (INMIC). 2020; 1–6. https://doi.org/10.1109/inmic50486.2020.9318106
33. Farhan RI, Maolood AT, Hassan NF. Performance analysis of flow-based attacks detection on CSE-CIC-IDS2018 dataset using Deep Learning. Indones J Electr Eng Comput Sci. 2020; 20(3): 1413–1418. https://doi.org/10.11591/ijeecs.v20.i3.pp1413-1418
34. Sarhan M, Layeghy S, Moustafa N, Portmann M. NetFlow datasets for Machine Learning-based network intrusion detection systems. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham: Springer; 2021; 117–135. https://doi.org/10.1007/978-3-030-72802-1_9
35. Argus. Openargus. [Online]. Retrieved February 20, 2023, from https://openargus.org/
36. Scikit learn. Sklearn.preprocessing: Standard Scaler. [Online]. Retrieved February 20, 2023, from https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.StandardScaler.html
37. Scikit learn. Sklearn.preprocessing: Power Transformer. [Online]. Retrieved February 20, 2023, from https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.PowerTransformer.html
38. Jiang H, Lin J, Kang H. FGMD: A robust detector against adversarial attacks in the IOT network. Future Gener Comput Syst. 2022; 132: 194–210. https://doi.org/10.1016/j.future.2022.02.019.

39. Scikit learn. Sklearn.preprocessing: OrdinalEncoder. [Online]. Retrieved February 20, 2023, from https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.OrdinalEncoder.html
40. Brownlee J. (2021 Mar 16). SMOTE for imbalanced classification with python. [Online]. Machine Learning Mastery. Retrieved February 20, 2023, from https://machinelearningmastery.com/smote-oversampling-for-imbalanced-classification/
41. PyPI. Imblearn. [Online]. Retrieved February 20, 2023, from https://pypi.org/project/imblearn/
42. Wang W, Du X, Wang N. Building a cloud ids using an efficient feature selection method and SVM. IEEE Access. 2019; 7: 1345–1354. https://doi.org/10.1109/access.2018.2883142
43. Moon D, Im H, Kim I, Park JH. DTB-ids: An intrusion detection system based on decision tree using behaviour analysis for preventing apt attacks. J Supercomput. 2015; 73(7): 2881–2895. https://doi.org/10.1007/s11227-015-1604-8
44. Nayak J, Meher SK, Souri A, Naik B, Vimal S. Extreme learning machine and bayesian optimization-driven intelligent framework for IOMT cyber-attack detection. J Supercomput. 2022; 78(13): 14866–14891. https://doi.org/10.1007/s11227-022-04453-z
45. Kumaran SS, Balakannan SP, Li J. A deep analysis of object capabilities for intelligence considering wireless IOT devices with the DNN approach. J Supercomput. 2021; 78(4): 4745–4758. https://doi.org/10.1007/s11227-021-04064-0
46. Mishra S. An optimized gradient boost decision tree using enhanced African buffalo optimization method for cyber security intrusion detection. Appl Sci. 2022; 12(24): 12591. https://doi.org/10.3390/app122412591
47. Mantas CJ, Castellano JG, Moral-García S, Abellán J. A comparison of random forest-based algorithms: Random credal random forest versus oblique random forest. Soft Comput. 2018; 23(21): 10739–10754. https://doi.org/10.1007/s00500-018-3628-5
48. PyTorch. Adam. Adam - PyTorch 1.13 documentation. [Online]. Retrieved February 27, 2023, from https://pytorch.org/docs/stable/generated/torch.optim.Adam.html
49. Sirignano J, Spiliopoulos K. Scaling limit of neural networks with the Xavier Initialization and Convergence to a global minimum. arXiv:1907.04108v3 [math.PR]. 2022 Apr 12. arXiv.org. Retrieved February 27, 2023, from https://arxiv.org/abs/1907.04108v3
50. PyTorch. What is torch.nn really? PyTorch Tutorials 1.13.1+cu117 documentation. [Online]. Retrieved February 20, 2023, from https://pytorch.org/tutorials/beginner/nn_tutorial.html
51. Scikit learn. Sklearn.model_selection: train_test_split. [Online]. Retrieved February 20, 2023, from https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.train_test_split.html
52. Dina AS, Siddique AB, Manivannan D. A deep learning approach for intrusion detection in internet of things using focal loss function. Internet Things. 2023; 22: 100699. https://doi.org/10.1016/j.iot.2023.100699
53. Gupta K, Sharma DK, Datta Gupta K, Kumar A. A tree classifier-based network intrusion detection model for internet of medical things. Comput Electr Eng. 2022; 102: 108158. https://doi.org/10.1016/j.compeleceng.2022.108158
54. Chaganti R, Mourade A, Ravi V, Vemprala N, Dua A, Bhushan B. A particle swarm optimization and deep learning approach for intrusion detection system in the internet of medical things. Sustainability. 2022; 14(19): 12828. https://doi.org/10.3390/su141912828
55. FiratKilincer I, Ertam F, Sengur A, Tan R-S, Rajendra Acharya U. Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. Biocybern Biomed Eng. 2023; 43(1): 30–41. https://doi.org/10.1016/j.bbe.2022.11.005.

