Journal of Applied Engineering and Technological Science
Vol 7(1) 2025: 745-761

A COMPREHENSIVE REVIEW OF DEEP LEARNING TECHNIQUES FOR INTRUSION DETECTION IN THE INTERNET OF MEDICAL THINGS

Aisha Essa Mohammad[1*], Amer Abdulmajeed Abdulrahman[2]
Computer Science Department, College of Science, University of Baghdad, Baghdad, Iraq[12]
aaesha.eesa2201m@sc.uobaghdad.edu.iq[1], amer.abdulrahman@sc.uobaghdad.edu.iq[2]

Received: 27 November 2024, Revised: 15 May 2025, Accepted: 12 August 2025
**Corresponding Author*

ABSTRACT
The work revisits the security issues of Internet of Medical Things (IoMT) platforms and provides a list of deep learning models used for intrusion detection. The study fills the salient gap in early detection of actual IoMT system intrusions for enhanced medical device and data security. A wide-ranging and systematic investigation of deep learning models, such as CNNs, LSTMs, and hybrid ones (GNNs and BiLSTMs) recently introduced was carried out. These were then analyzed against well-known benchmark datasets, such as ToN-IoT and IoT-Healthcare Security and WUSTL-EHMS-2020, to consider the quality of their detection work on cybersecurity threats for IoMT systems. The results indicated high accuracy in cyber threat detection, reaching even 100% accuracy. But the challenges are still how to decrease false positives and improve the real-time performance of the model on robustness and generalization when making real-world applications. The research is literature-based and aimed to provide some further updates on a secure IoMT framework by identifying recent studies in the security of the IoMT ecosystem and shedding light on future work using hybrid methods, blockchain technology, or federated learning approaches that can contribute to the detection of IDSs. And all can help pave the way for a more secure, privacy-protecting IoMT that safeguards extremely sensitive medical data. The research also enhances the model: utilizing 15+ deep-learning models to propose an IoMT-resistant architecture. This can promote participation in the theoretical research and practical security protocols in the IoMT context, thus drawing attention and comprehension from researchers and practitioners to enhance security protocols.
Keywords: *Internet of Medical Things (IoMT)**,** Intrusion Detection Systems (IDS), Deep Learning (DL).*

1. Introduction

The evolution of the Internet of Medical Things (IoMT) has revolutionized how data in healthcare is collected, processed, and exploited. Such an IoMT will enable linking up of wearable sensors, let along the diagnostics devices and cloud-based platforms to promote continuous remote monitoring, real-time diagnostics, and intelligent health analytics. The IoMT market value is estimated to be approximately $230.69 billion globally in 2024, and it is forecasted to grow at a CAGR of 18.2% reaching over $658.57 billion by 2030 Mpembele (2024).

This exponential growth is mainly due to the increasing trend of remote patient monitoring systems, wearable medical devices, and telemedicine Razzaq et al. (2024). Further, the IoMT delivers concrete and precise medical information that speeds up the treatment process, reduces error possibilities in medication, and diagnoses early-stage diseases. It can help with a more rapid diagnosis and also enhance patient satisfaction. Changing from a curative to a preventive focus on healthcare increases the quality of care for patients, with positive effects on stakeholders such as insurance or pharmacies. IoMT also has the advantages of providing access to medical information to nurses and patients' families from a remote location. It eradicates the necessity of visiting hospitals frequently, reduces expenses, conserves resources, and prevents COVID-19 from transmitting.

Additionally, patients can be treated in their preferred habitat, which is home. Overall, the IoMT is a significant advancement in technology that could have a substantial impact on healthcare services, both for patients and providers Si-Ahmed et al. (2023). Despite the advantages above, IoMT is vulnerable to a serious presence of cybersecurity issues. These devices handle critical, sensitive information, making them a high-value target for hackers. Studies have demonstrated that 99% of healthcare organizations have devices that are susceptible to exploitation, including the IoMT Park et al. (2019).

Nowadays, connected medical devices are considered one of the top five most harmful components of a network that is devoted to business Oh et al. (2023). Traditional ML-based conventional IDSs have not been effective in protecting the IoMT ecosystem. Zero-day attacks, skewed data, dimensional spaces, and mutability of medical traffic in the network are usually a problem for them, Nakıp & Gelenbe (2024). Such constraints result in low sensitivity of clinical results and an inability to respond in a real-time setting. Due to the above issues, deep learning (DL) has gained popularity in generating complex and versatile IDS. Models like Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and hybrid combinations such as Graph Neural Networks (GNNs) with BiLSTM have proven capable of extracting complex temporal and spatial patterns. This has enabled the proper identification of threats in healthcare institutions. This has been achieved through integrating techniques suitable for detecting threats in the care facilities Ravi et al. (2023).

Additionally, the association of blockchain with federally-based education has demonstrated the potential for enhancing the safety and integrity of medical data in distributed environments Wang et al. (2022). Adversarial modification of these devices can have serious consequences, such as an overdose of insulin or the remote activation of pacemakers, as these devices are directly related to patients' lives. Attacks on online medical devices could lead to serious bodily injury and life-threatening effects for the individuals involved. For instance, malicious code in medical insulin pumps may lead to patients receiving too much insulin, which would lead to death. Patients' lives can potentially be in jeopardy when a pacemaker or other connected cardiac equipment is hacked. Researchers have demonstrated several assaults on medical devices, such as denial-of-service attacks, message manipulation, eavesdropping, and bogus data injection, which can jeopardize patient security, safety, and the availability of vital systems Yaqoob et al. (2019), Gatea & Hameed (2022).

This article presents a comprehensive analysis of over 15 DL-based IDS models that were evaluated across more than ten different benchmark datasets. To the knowledge of the authors, this is the first study that compares multiple different models and configurations. The GNN-BiLSTM architecture is found to be the topper in terms of both accuracy and generalizability. Current issues in research work are identified, future research directions suggested, and the article is intended to provide an important reference for researchers and practitioners to enhance the security of their IoMT systems by using smart intrusion detection.

The organization of the article is outlined as follows: Section 2 presents a survey on ID model development for the Internet of Medical Things employing deep learning methods, including subsections. Section 3 discusses the problems and unanswered questions. Section 4 presents the detection models in subsections. Section 5 introduces the chosen methodologies. Section 6 presents the results and discussion, where IoMT intrusion detection studies are compared conceptually. Section 7 concludes the paper and outlines future work.

2. Literature Review

The articles were chosen through a systematic searching process, such as IEEE Xplore, Springer, Science Direct, and Scopus. Search queries including IoMT, fraud detection, deep learning, and hybrid IDS were used. Research scheduled to be conducted from 2022 through 2025 was chosen to increase the currency and relevance of the review. Only papers peer-reviewed by the Journal and with a high impact on the conference were considered. Current literature would improve the quality of the paper and give it a better scientific basis and outlook.

With the trend of Internet of Medical Things (IoMT) having developed rapidly from 2022 to 2025, traditional Machine Learning (ML) models, deep learning (DL), and hybrid methods contribute massively. This section presents the main concepts, that is, models and challenges in intrusion detection for IoMT, draws us to review current related work, and opens new doors. It also presents a short summary of the major related works on intrusion detection for Internet of Medical Things, especially the research that has employed deep learning methods.

2.1 Traditional ML

First works on intrusion detection in the IoMT used machine-learning (ML) techniques such as Support Vector Machines (SVM), Decision Trees (DT), and ensemble methods like

Random Forests (RF). These basic techniques have difficulty in handling high-dimensional, nonuniform, and dynamic feature data that commonly exists in IoT scenarios.Dadkhah et al. (2024) applied ML techniques (such as Logistic Regression, AdaBoost, Random Forest, and Deep Neural Network (DNN).

The evaluation is dedicated to three different purposes: binary classification (i.e., Benign and Attack), Categorical classification (i.e., benign, spoofing, DDoS, DoS, recon, and MQTT), and multiclass classification (i.e., all other available classes). Shambharkar & Sharma (2023) proposed three deep learning models: Linear Support Vector Machine (LinSVM), Convolutional Support Vector Machine (ConvSVM), and Categorical Embedding (CatEmbedding), along with seven machine learning models that will be used to develop an intrusion detection system for Internet of Things (IoMT) networks.

2.2 Deep Learning Models

Akar et al. (2025) suggested a new way to recognize various attacks that target the Internet of Medical Things (IoMT) devices. This would utilize an enhanced version of the LSTM deep learning algorithm. In their article, Barnawi et al. (2024) proposed a framework that combines Federated Learning (FL) and Differential Privacy (DP) to enhance the privacy and safety of data in the Internet of Medical Things (IoMT). By combining the decentralized approach of FL with the protection against data re-creation of DP, the framework guarantees data secrecy. The framework is employed to create Convolutional Neural Networks (CNNs) that are capable of recognizing tuberculosis from chest X-ray datasets. The evaluation demonstrates that the framework is superior to simple models lacking security, making it a powerful solution for secure and private healthcare applications. It uses seven models on three datasets, with accuracy values for each model in every dataset, as shown in Table 1.

Table 1 - Federated Learning (FL) and Differential Privacy (DP) with seven models on the three datasets and accuracy.

Dataset name	VGG19	InceptionResNetV2	VGG16	InceptionV3	MobileNet	DenseNet121	ResNet50
Dataset 1 (Shenzhen Chest X-ray)	77.46%	77.46%	78.16%	78.16%	81.69%	77.46%	53.52%
Dataset 2 (Montgomery County Chest X-ray)	64.28%	64.71%	67.85%	60.71%	57.14%	53.57%	42.85%
Dataset 3 (Tuberculosis Chest X-ray)	76.00%	84.00%	74.50%	82.50%	95.00%	84.00%	68.00%

MobileNet performed consistently well across all three datasets, with the highest accuracy on Dataset 3 (95%), ResNet50 performed poorly across all datasets, with accuracy below 42.85%. Rbah et al. (2023) introduced an intrusion detection system (IDS) using deep learning techniques, like LSTM, CNN, and GRU, to identify attacks in IoMT fog environments. The CNN model reduces detection time and memory usage, achieving an accuracy of 99.62%. Vaisakhkrishnan et al. (2024) evaluated four models—CNN, Autoencoder (AE), Transformer Network, and LSTM—and found that the LSTM Network demonstrates exceptional performance in intrusion detection. Revathi et al. (2024) proposed ParticleSwarmNetGuard (PS-NG), a novel IDS that utilizes deep learning to enhance security in IoMT devices. PS-NG surpasses current data security standards with an accuracy of 96%.

Kamil & Mohammed (2023) proposed an IDS infrastructure between end devices, utilizing CNN and the UNSW-NB15 dataset. The goal is to improve network security by detecting new threats that challenge traditional detection systems and firewalls. Alalhareth & Hong (2023) proposed a fuzzy-based self-tuning LSTM model for IoMT intrusion detection. The model demonstrates higher detection rates, lower false positive rates, and excellent precision in

comparison to traditional methods. Daher (2023) analyzed healthcare datasets and developed IDS models that combine deep reinforcement learning (DRL) with Q-learning and traditional ML approaches, achieving a high accuracy rate exceeding 92%. Judith et al. (2023) combined Principal Component Analysis (PCA) with deep learning for IoMT. This approach is particularly beneficial for quickly notifying healthcare officials about intrusions, thereby improving the effectiveness of healthcare services. Ravi et al. (2023) employed the flow of network information and patient biometrics to derive the most effective features from a global attention layer. Their methodology achieves a 95% success rate with network-related features, an 89% success rate with biometrics, and a 99% success rate with all features. This is superior to the currently popular methods. Fouda et al. (2022) proposed a sub-class intrusion detection system that employs a deep sub-class distribution of OSVMs (Deep SDOSVMs). The dynamic autoencoder model (DynAE) is utilized to generate additional instances of the same class. This improves the performance of the classification and overcomes the limitations of traditional cluster analysis when evaluated on the ToN_IoT dataset. Vijayakumar et al. (2023) suggested a deep neural network-based approach to identify cyber-attacks in the Internet of Health Things (IoHT) system. This system has an average accuracy of 99.85% and a false positive rate of 0.01.

2.3 Hybrid DL Models

Berguiga et al. (2025) outlined a hybrid intrusion detection system based on deep learning designed for application in Internet of Medical Things (IoMT) networks. This system incorporated CNNs to extract features and LSTMs to make follow-up predictions. It uses fog computing on a Raspberry Pi to distribute processing over a wider area, enhancing responsiveness. The model will achieve high accuracy levels, precision, recall, and F1-scores in identifying attacks such as DDoS, making it more accurate than the old methods.

Rbah, Mahfoudi, Fattah, Balboul, Mazer, et al. (2024) described a hybrid deep learning strategy for the security of IoMT that combines Graph Neural Networks (GNNs) and Bidirectional Long Short-Term Memory Networks (BiLSTMs). The method achieves a high degree of success and provides a rapid response time, effectively addressing current flaws when evaluated using the IoT-Healthcare security dataset.

Okpu et al. (2024) combined Feedforward Neural Networks (FNN) and fuzzy logic to propose a hybrid method for recognizing intrusion in healthcare-connected devices. This method effectively combines the benefits of both models to increase security. Alzubi et al. (2024) introduced a hybrid deep learning platform that combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. The framework is intended to recognize new perpetrators and preserve healthcare data effectively. Fadhil et al. (2024) developed a hybrid CNN-LSTM algorithm that utilizes the Lion optimization algorithm (LOA) and the Grey Wolf optimization algorithm (GWO) to achieve a prediction accuracy of 99.26%, surpassing the current methods that are employed globally. Kamil & Mohammed (2023) presented an IDS that employs a hybridized CNN as well as dense layers, and compares this to Naïve Bayes (NB) machine learning methods. The hybrid CNN model had greater success in experiments with the UNSW-NB15 dataset. Wang et al. (2022) integrated Blockchain technology with Deep Neural Networks (DNNs) to perform anomaly detection in IoMT systems. Blockchain is utilized for secure data sharing, while DNN models ensure accurate anomaly detection.

3. Connected Healthcare Challenges

Cyber-attacks on connected healthcare equipment pose a significant threat to patient privacy and health, making it crucial to ensure high safety attributes that protect the confidentiality and integrity of patient health data. Any alteration to this data can adversely affect patient treatment, potentially leading to severe consequences in emergencies. IoMT systems have security problems because of hardware, software, and network limitations. Practical security steps need to be implemented to fix these problems and lower the risks Vaisakhkrishnan et al. (2024), Alalhareth & Hong (2023).

4. Intrusion Detection Model

Most studies adopt a model that involves intrusion detection, which comprises many steps, as shown in Fig. 1 below:

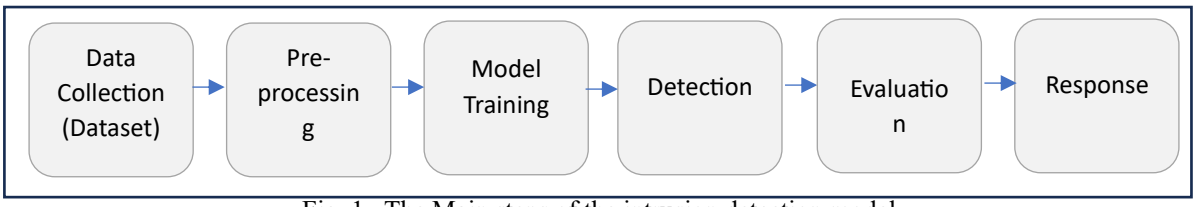

Fig. 1. The Main steps of the intrusion detection model

4.1 Datasets for Intrusion Detection Models

This subsection is dedicated to reviewing the datasets used to detect the Intrusion for IoMT.

The CICIoMT2024 Dataset is a realistic benchmark dataset used by Dadkhah et al. (2024) and Akar et al. (2025) to facilitate the development and evaluation of internet-based medical safety solutions. To accomplish this, 18 attacks were carried out against a testbed for the IoMT composed of 40 devices (25 real devices and 15 simulation devices), considering the plurality of protocols employed in healthcare (e.g., Wi-Fi, MQTT, and Bluetooth). The UNSW Canberra IoT Labs and the Cyber Range designed the ToN-IoT dataset. It was used by Vaisakhkrishnan et al. (2024), Fouda et al. (2022), Okpu et al. (2024), Alanazi et al. (2023), and Awotunde et al. (2021) to evaluate their models.

The NF-TON-IoT Dataset used by Saran & Kesswani (2024) is a collection of network flow data intended for detecting intrusions in IoT networks. It contains data on network traffic from IoT devices, focusing on recognizing criminal and anomalous behavior in the network. The dataset includes both typical and unusual traffic patterns, providing a broad spectrum of attacks, particularly network-based ones. It is typically employed to create and evaluate intrusion detection systems utilizing machine learning and deep learning methods. The information is gathered from actual IoT networks, which makes it ideal for practical cybersecurity research in these networks. Another dataset, the IoT-Healthcare security dataset, was introduced by Rbah, Mahfoudi, Fattah, Balboul, Mazer, et al. (2024), Rbah et al. (2023), Daher (2023), Rbah, Mahfoudi, Fattah, Balboul, Chetioui, et al. (2024) to validate their method.

The WUSTL-EHMS-2020 dataset was used by Alalhareth & Hon (2023), Judith et al. (2023), and Shambharkar & Sharma (2023). The source of this dataset is a real-time testbed for the Enhanced Healthcare Monitoring System (EHMS). The four basic components of the testbed are: the medical monitoring sensors, the data-transmitting gateway, the network infrastructure, and the control unit with viewing capabilities. Patient-attached sensors deliver data through the gateway to a dedicated server, where routing and switching algorithms visualize the information. The dataset's limitations affect the generalizability of the information, but do not specifically mention the lack of pediatric data.

The CICIDS 2017 dataset was used by Ramya et al. (2023), Manimurugan et al. (2020), and Abdualrahman & Ibrahem (2021). This dataset provides a comprehensive set of network traffic data, enabling the training of deep learning algorithms to identify anomalies and potential threats specific to medical devices. By leveraging these techniques, researchers can enhance the security of IoMT systems, effectively detecting emerging and unknown attacks that target sensitive medical data and devices.

The dataset of intrusion incidents utilized by Ravi et al. (2023) demonstrated a higher success rate with the proposed model in the network monitoring tool, aimed at protecting healthcare and medical sector computers and networks from intrusion.

Wang et al. (2022) utilized two datasets constructed using the traffic anomaly detection framework (TADA and TADB), the latter of which collects data within the IoMT-blockchain network. The ECU-IoHT dataset used by Vijayakumar et al. (2023) contains 111,207 samples, including normal and various other types of attacks, such as ARP-Spoofing, DoS attacks, Nmap Port Scan, and Smurf attacks.

For Tsimenidis et al. (2022), two different types of profiles from the CSE-CIC-IDS 2018 general dataset were employed to assess the proposed model. The Canadian Institute for Cybersecurity Intrusion Detection System of 2017 (CICIDS 2017) and the UNSW-NB15 are the two datasets used to evaluate the model's effectiveness. The dataset is owned by Alhijaj et al. (2021). The MQTT-IOT-IDS2020 dataset was employed by Memon et al. (2023) As a benchmark, the particle swarm optimization (PSO) algorithm is employed to determine the optimal features from the dataset.

The effectiveness of 10 different machine learning (ML) methods is assessed. The outcomes demonstrate high classification accuracy, ranging from 97% to 99%. LIME theories have been used to explain why humans have the capacity to understand the meaning of the most successful model. Three publicly accessible data sets (WUSTL-EHMS-2020, IoTID-20, and WUSTL-IIOT-2021) were used by Alalhareth & Hong (2024) to assess their technique. Impressively low misclassification rates of 0.0042%,0.0006%, and 0.00004%, respectively, are paired with excellent accuracy rates of 99.57%, 99.93%, and 99.99% for signature-based detection and 99.47%, 99.98%, and 99.99% for anomaly-based detection.

4.2 Pre-processing

Pre-processing is enhancing data quality before a deep learning model is used. It includes data cleaning, normalization, feature extraction, segmentation, encoding, and transformation. This process improves model accuracy, reduces noise, accelerates training, and handles diverse IoMT data. Wang et al. (2022) used Normalization Standardizes the input data so that all values have the same scale, which is typically accomplished through methods like Min-Max scaling or Z-score normalization. It facilitates the model's learning by preventing larger-scale features from significantly impacting the process. Additionally, it uses Feature Extraction to employ methods like the multi-model autoencoder (MMAE) to harvest important information from raw data. This involves extracting low-level features of fusion and temporal structure from traffic in the network, which significantly reduces the complexity of the data.

Kamil & Mohammed (2023) normalized the data by taking each feature and converting it to a range of [0, 1]. This will ensure the data is consistent, reduce the time needed to train machine learning algorithms, and transform raw data into useful features using Convolutional Neural Networks (CNN). It entails extracting the most important patterns, reducing their dimensionality through aggregation, and utilizing activation functions to enhance the model's performance.

Fadhil et al. (2024) scaled the data to ensure all features are within a specific range. This prevents most of the data from being affected by any single feature, thereby improving the model's efficiency. Uses the Lion Optimization Feature Selection (LOFS) algorithm to identify and choose the most significant features for intrusion detection. This algorithm reduces the dimensionality of the data and increases the accuracy of the model.

For Ravi et al. (2023), one-hot encoding is employed to convert categorical traits into numerical values. Only numerical characteristics are used in the model, while five important features (typically, source and destination packets, protocol type, and length) are gathered from the dataset for further analysis. Fouda et al.'s work in (2022) involved scaling data using Min-Max normalization to ensure efficient training, utilizing deep learning models like autoencoders and BiLSTM for learning and extracting hierarchical features. Alzubi et al. (2024) used Min-Max normalization to ensure features are scaled within a [0, 1] range. Feature extraction is accomplished using CNNs and LSTMs that are accurate at recognizing patterns. In the work of et al. (2024) Normalization Scales have a range of 0 to 1; the lower the value, the smaller the range. Convolutional Neural Networks (CNNs) automatically gather important information from medical data (e.g., chest x-rays). The procedure also employs Differential Privacy to safeguard critical information by adding noise during the extraction of features, ensuring privacy in federally educated environments. In the study of Rbah, Mahfoudi, Fattah, Balboul, Mazer, et al. (2024), Min-max scaling was employed to standardize the feature vectors. These vectors must be within a specific range (e.g., between 0 and 1). Features were derived from the "IoT healthcare security" dataset using a combination of the Chi-squared Test and Label Encoding that was intended to ensure the efficient representation of categorical variables.

The method of Dadkhah et al. (2024) normalized the data for each attribute by converting the lowest value to a decimal number between 0 and 1. This technique facilitates the data's understanding and reduces the time needed to train. Feature Extraction is the process of obtaining the following essential information from network traffic: Protocol Specification: It describes the various protocol types (e.g., Wi-Fi, MQTT, Bluetooth). Packet-Level Specification: The length of packets, their flags (SYN, ACK, FIN), and the number of packets (e.g., ICMP, DNS). Traffic Dynamics: It captures the transmission rates, time-to-live TTL, and the variance of packet lengths.

Berguiga et al. (2025) utilized Min-Max normalization to convert the features into a scale from 0 to 1. This normalization method ensures that the model is not adversely affected by the larger-scale features, such as "Flow_IAT_Mean", in comparison to "Fwd_Header_Len". The CNN model was employed to extract features. Convolutional layers were used to identify the most essential patterns in the data, helping the model concentrate on the most important features for classification. In the work of Alalhareth & Hong (2023), Min-Max normalization was employed to convert attribute values between 0 and 1. This normalized the effect of large values while preventing the model from having a specific bias towards one particular feature. Feature Extraction is concerned with: Identifying the features of network traffic (e.g., packet size, protocol composition) and obtaining information about the patient's biometric features (e.g., heart rate, blood pressure). A global attention mechanism will focus on the most critical aspects of both data types to improve the detection of intrusion.

In their work, Akar et al. (2025) employed Data normalization to convert feature values into a comparable scale. This is crucial to distance-based and gradient-based classification methods. This guarantees that the LSTM model will have an effective way to learn from the data. The paper employs LSTM to automatically extract temporal features from time-series data, crucial for detecting complex patterns in IoMT network traffic. Features, such as packet size, flow duration, and protocol types, are considered necessary.

For Shambharkar & Sharma (2023) StandardScaler calculated the average as zero and the standard deviation as one, which normalizes any features that are skewed. The Covariance Matrix is employed to eliminate features that are irrelevant or highly associated, and Ordinal Encoding is used to convert categorical data into its associated ordinate. In the study conducted by Vaisakhkrishnan et al. (2024) regarding StandardScaler, data were standardized with a mean of 0 and a standard deviation of 1. One-Hot Encoding: Transforms categorical variables into binary vectors that can be used to classify multiple classes. Label Encoder: Categorical variables are converted into labels that are integers. Data Transformation purges features that are not relevant and removes data that is mixed up.

In the study conducted by Judith et al. (2023) Regarding StandardScaler, data was rescaled to have a mean of 0 and a standard deviation of 1. Encoding of labels: converts categorical information into numerical values. PCA (Principal Component Analysis): Reduces the dimensionality of the data by taking a smaller set of uncorrelated features. In the work of Daher (2023) regarding StandardScaler, the method distributes data across a range of values with a mean of 0 and a standard deviation of 1, ensuring consistent data distribution and recovering important information for training deep-Q learning-based intrusion detection.

According to Revathi et al. (2024), Scaling converts the data into a normal distribution, which ensures the data's uniformity across features. This facilitates the improvement of the performance of machine learning and deep learning models by ensuring that all of the input values are in the same range. PSO (Particle Swarm Optimization) selects important features from network traffic and patient data, which improves the accuracy and speed of predictions. CNN: Recovered patterns from traffic patterns and patient data, which enhanced the detection of attacks.

4.3 Deep Learning Algorithms

Deep learning approaches are becoming increasingly popular in intrusion detection for the Internet of Medical Things (IoMT) because of their capacity to handle huge and complex data sets. The most popular techniques consist of: Convolutional Neural Networks (CNNs), which are extensively employed to analyze spatial data, including structured data from different medical devices. When CNN is combined with techniques such as Long-Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), or reinforcement learning, the strengths of each algorithm are

leveraged to enhance the system's ability. The LSTM, CNN, and GRU used by Rbah et al. (2023) and Vaisakhkrishnan et al. (2024) focused on four different models: CNN, Autoencoder, Transformer Network, and LSTM Network. Integrates Software Defined Network (SDN) controllers with deep learning methodologies, employing Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (Bi-LSTM) networks as referenced in Rbah, Mahfoudi, Fattah, Balboul, Chetioui, et al. (2024). Moreover, in 2024, a hybrid model was presented by Rbah, Mahfoudi, Fattah, Balboul, Mazer, et al. (2024), introducing a hybrid deep learning (DL) approach for IoMT security. The framework leverages a Graph Neural Network (GNN) and Bidirectional Long-Term Memory (Bi-LSTM) network for efficient and timely cyber threat detection within the IoMT system. The fuzzy-based self-tuning (LSTM) model was introduced, where the model produced robust detection capabilities, minimal false positive rates, and high accuracy Alalhareth & Hong (2023). In 2024, a novel intrusion detection system called ParticleSwarmNetGuard (PS-NG) was introduced by Revathi et al. (2024). This system combines a Deep Neural Network structure and Element Swarm Optimization to provide a reliable solution intended for the Internet of Medical Things (IoMT). Using a testing dataset to forecast typical or non-standard assaults, the DNN (Deep Neural Network) model extensively tests the DNN-based attack detection system, as described by Vijayakumar et al. (2023). Three DL models are adopted, including AE, CNN, and LSTM, used by Sulaiman et al. (2024).

5. Methodology

In this section, we discuss the reasons for specific approaches, as well as the participants, the data gathered, the instruments employed, and the method selected. The method of utilizing Deep Learning (DL) models, particularly Convolutional Neural Networks (CNNs) and Graph Neural Networks (GNNs), was chosen because of their high efficiency in recognizing intrusions in the Internet of Medical Things (IoMT) environment. Deep learning models can deal with the large volume and complexity of data associated with medical IoT devices; these devices include sensors, traffic, and biometrics from patients Rbah, Mahfoudi, Fattah, Balboul, Mazer, et al. (2024). CNNs were selected because of their propensity to recognize patterns in data, which is crucial to the understanding of the behavior of network traffic and sensor data in IoMT systems Revathi et al. (2024). GNNs were chosen because of their capacity to represent the complex relationships between connected IoMT devices. This is crucial to recognizing attacks based on the network Vaisakhkrishnan et al. (2024). Models like GNN-BiLSTM were chosen to have both temporal and spatial properties in the IoMT dataset, which enhances the accuracy of the model and its generalizability Shambharkar & Sharma (2023).

The participants are considered to be IoMT devices and communication systems Shambharkar & Sharma (2023). These devices include wearable sensors, patient monitoring devices, and medical equipment that generate information about the patient's health and network activity Revathi et al. (2024). The information attained includes network data regarding traffic, patient biometrics, and sensor data (e.g., heart rate, blood pressure, and temperature) Vaisakhkrishnan et al. (2024). The IoMT devices are diverse: there are intelligent vests, patient monitors that are connected, and various medical sensors Shambharkar & Sharma (2023). Devices have different abilities in terms of computational power, memory, and data generation frequency, all of which may have an effect on the performance of detection models Revathi et al. (2024).

Data that will be gathered, such as Network Traffic Data, contains the sizes of packets, the duration of flow, and the protocol types, which are all derived from the Internet of Things Rbah, Mahfoudi, Fattah, Balboul, Mazer, et al. (2024). Patient Biometric Data: This data includes the heart rate, blood pressure, ECG readings, and other physiological information derived from IoMT instruments Vaisakhkrishnan et al. (2024).

Attack Data: Information regarding known and proposed cyberattacks on IoMT systems, including DDoS attacks, man-in-the-middle attacks, and ECG-based spoofing Shambharkar & Sharma (2023). The instruments used in Graph Neural Networks (GNNs) are employed for the reason that they can represent device configurations and recognize errors Vaisakhkrishnan et al. (2024). In Convolutional Neural Networks (CNNs), they are used to pattern-spotify data from both network traffic and sensor information Revathi et al. (2024).

In BiLSTM (Bidirectional LSTM): Data that is time-series, such as patient biometrics Rbah, Mahfoudi, Fattah, Balboul, Mazer, et al. (2024). In Particle Swarm Optimization (PSO), it is used for feature selection, to optimize the choice of relevant features, and to increase the accuracy of the model Shambharkar & Sharma (2023). The evaluation metrics use the accuracy, precision, recall, and F1-score to determine their effectiveness Revathi et al. (2024).

6. Results and Discussion

The deep learning models evaluated in this study demonstrated a significant capacity to recognize cyber criminals in the Internet of Medical Things (IoMT) context. The results indicate several beneficial aspects of the system and areas for improvement, each contributing to the continued development of IDSs for medical networks.

One of the most significant strengths of this research is the effective comparison in Table 1, which contrasts the performance of various deep learning models in terms of their accuracy and dataset appropriateness. The results clearly demonstrate the superiority of models like Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and their combination with BiLSTM over traditional machine learning methods, particularly in detecting threats in real-time medical systems. The models were evaluated across multiple datasets, including ToN-IoT and IoT-Healthcare Security, both of which demonstrated their resilience in diverse IoMT environments.

However, the investigation also mentions some practical issues that still influence the effectiveness of these models. Specifically, problems with false positives still constitute a significant obstacle. Despite the high accuracy of some models (up to 100%), the false alarm rate in specific models, especially those not optimized for the IoMT, is still problematic. These issues are exacerbated by real-time systems with low latency, which is crucial for the immediate detection and prevention of injury.

A closer study of the models reveals that optimizing specific domains has positively impacted the individual system compared to others. As an example, the GNN-BiLSTM, which is a hybrid approach that unifies the advantages of the spatial and temporal feature extraction models, achieves a high level of success in terms of accuracy and generalizability (it has an accuracy rate of 99.98%). This is more beneficial than the usual implementation in IoT intrusion detection, which is significantly less accurate due to its broader range of use and specialization in the IoT field.

As an illustration, models detailed in Okpu et al. (2024) demonstrated that specifically created systems that could be offered to IoMT bear a better success rate than the general models since standard systems bear 92 percent accuracy, but 99.98 percent is what characterizes the case of specifically created systems that are presented to the IoMT. It is seen that intrusion detection systems need to be tailored to the unique characteristics of medical tools and healthcare facilities. In these settings, threat detection must be rapid and error-free, as it is of paramount concern to patient safety. Additionally, the analysis indicates that hybrid models like CNN-LSTM have 99% accuracy to 1 millisecond latency, making them ideal for deploying in real-time healthcare apps. This hybrid model's capacity to handle large amounts of data while maintaining efficiency is beneficial for addressing the security concerns arising from IoMT devices.

Similar to other innovations, these findings indicate that there should be consistent evolution. Even though the CNN-GRU model has an impressive accuracy of 99.62%, it suffers from a high memory consumption of 2.1GB, which may impede its use in constrained edge devices with limited resources. This discrepancy has been surmounted in newer models, such as lightweight LSTMs that are designed to lower memory consumption while still maintaining accuracy.

The ongoing conflict is increasing the complexity of models aimed at reducing false positives and enhancing device capacity in the real world of IoT, where devices vary in power, storage, and data generation frequency. Adversities like network congestion and ensuring the system is practical are crucial to providing adequate real-time protection for important healthcare information. Ultimately, although deep learning-based IDS models have significantly enhanced detection effectiveness, additional research is necessary to make the models more efficient, reduce false positives, and ensure they are effective across different devices and scenarios. Plans include

utilizing blockchain technology to augment federated educational tools to enhance data security and system permanency. Also, more specialized data is necessary to describe the various configurations of medical devices and the dangers of cyberspace in healthcare.

Overall, the investigation's findings demonstrate the beneficial nature of deep learning-based IDS models for the IoMT system. Models dedicated to the IoMT have a higher degree of success than general-purpose IoT-based intrusion detection systems. This is illustrated by a higher degree of accuracy and a lower percentage of false positives. While hybrids like CNN-LSTM offer a comprehensive approach balancing speed and accuracy, further optimization is needed to address resource constraints and enhance real-time detection capabilities. Future research is essential for strengthening the effectiveness and data safety of these systems, as well as improving their portability across a variety of devices. Future projects could explore the combination of blockchain technology and federally funded education to enhance data safety and privacy and to create more specialized datasets that represent the diverse configurations and issues in healthcare environments.

The studies covered in this paper are summarized and briefly compared in terms of datasets, methodology, limitations, comparative strengths, and the accuracy attained by the model. The values of the fields exhibiting the highest accuracy are indicated in bold, as presented in Table 2.

Table 2 - Comparison of Intrusion Detection on IoMT studies.

Authors and Year	Datasets	Methodology	Limitations	Comparative Strengths	Accuracy
Dadkhah et al. (2024)	CICIoMT 2024 Dataset	Logistic Regression (LR), Random Forest (RF), AdaBoost (AB), Deep Neural Network (DNN)	The evaluation is confined to lightweight creatures and standard procedures. The dataset includes only current IoMT devices; it ignores future planned improvements.	The dataset facilitates the recognition of multiple attacks and various IoMT devices. RF is superior to other technologies in numerous instances.	• Binary classification: • 99.6%. • Categorical (6-classes): 73.5%. • Multiclass (19-classes): 73%.
Shambharkar & Sharma (2023)	IoMT dataset with patient biometrics & network traffic flow	LinSVM (Linear SVM), ConvSVM (Convolutional SVM), CatEmbedding (Categorical Embedding)	The imbalance in the dataset is before resampling. The utilization of patient biometric information is innovative, but it necessitates a balanced sample population.	High accuracy compared to traditional IDS methods; a combination of biometric data and network flow	100%
Akar et al. (2025)	CICIoMT 2024 Dataset	LSTM (Long Short-Term Memory) with AdamW Optimizer	High computational resource usage; less suited for low-resource devices	Outperforms Logistic Regression and ANN for multi-class detection in IoMT	• Binary classification: • 100%. • Categorical (6-classes): 98%.

					• Multiclass (19-classes): 95%.
Rbah et al. (2023)	IoT-Healthcare Security dataset	LSTM, CNN, GRU	Challenges with implementing on IoMT devices, delay in attack detection in cloud-based solutions	Fog computing improves location awareness, mobility, scalability, low latency, and geographical distribution	CNN model: 99.62% accuracy
Vaisakhkrishnan et al. (2024)	IoMT (Internet of Medical Things) network traffic	CNN, Autoencoder, Transformer Network, LSTM	May struggle with evolving cyber threats, requiring continuous retraining and adjustment	The LSTM-based model achieved the highest performance in accuracy, precision, recall, and F1 score	LSTM: 97%
Revathi et al. (2024)	Network traffic and patient sensing data (IoMT datasets)	ParticleSwarmNet Guard (PS-NG), CNN, Swarm Optimization (PSO)	Device constraints (computing power and memory) limit traditional security methods.	PS-NG model with a combined dataset of network traffic and patient data for higher accuracy.	96%
Kamil & Mohammed (2023)	UNSW-NB15 dataset	CNN, SMOTE, BGMM, XGB, RFE	Challenges with class imbalance, computational complexity, and the difficulty of updating detection systems with new threats	Combines CNN for deep learning, SMOTE for data balancing, and BGMM for reducing bias in unbalanced datasets	• 98.80% for binary classification • 96.49% for multi-classification
Alalhareth & Hong (2023)	WUSTL-EHMS-2020 dataset (Network flow + patient biometric data)	Fuzzy-based Self-Tuning LSTM (Long Short-Term Memory)	Challenges with static epochs and batch sizes in traditional deep learning models	A dynamic early stopping mechanism using fuzzy logic to adjust patience, improving	The highest value of 0.966 was achieved for 25 features.

				detection accuracy	
Daher (2023)	Healthcare IoMT dataset	Deep Q-Learning (DQN), classical ML models (SVM, NN)	Challenges in adapting to large-scale data and ensuring real-time performance	DQN outperforms SVM and NN in accuracy, precision, recall, and F1 score	92.4%
Judith et al. (2023)	WUSTL-EHMS-2020 dataset	Multi-Layer Perceptron (MLP), KNN, SVM, Naive Bayes	Limited to man-in-the-middle attacks (e.g., spoofing, data injection) without covering other types	PCA-based feature reduction significantly enhances performance, and MLP performs best among classifiers	96.39% (MLP with PCA)
Ravi et al. (2023)	WUSTL EHMS 2020, SDN-IoT, KDDCup-99	CNN, LSTM, Attention Mechanism, Cost-Sensitive Learning	Dataset imbalance, some misclassifications, potential for overfitting on specific datasets	Combined features of network flow and patient biometrics, a cost-sensitive learning approach to handle data imbalance	99% (10-fold cross-validation) for IoMT dataset
Fouda et al. (2022)	ToN_IoT dataset	Deep SDOSVM (Deep Subclass Dispersion OSVM), DynAE (Dynamic Autoencoder)	Challenges with class imbalance and data dispersion in IoHT environments	Outperforms other one-class classifiers like OSVM and SVDD due to deep clustering and subclass dispersion	Above 97% AUC for the ToN_IoT dataset
Vijayakumar et al. (2023)	ECU-IoHT dataset	Deep Neural Network (DNN)	Dataset imbalance, real-time attack detection in IoHT can be challenging	Outperforms existing intrusion detection systems by achieving higher detection rates and lower false positive rates	99.85% (Accuracy), 0.99 AUC (Area Under ROC Curve), 0.01 (False Positive Rate)

Berguiga et al. (2025)	IoTID20, Edge-IIoTset datasets	CNN (Convolutional Neural Network), LSTM (Long Short-Term Memory)	Challenges related to IoMT network interconnectivity, real-time attack detection complexity	Hybrid CNN-LSTM model shows high performance in both binary and multiclass classification for attack detection in IoMT networks	99.92%
Rbah, Mahfoudi, Fattah, Balboul, Mazer, et al. (2024)	IoT Healthcare Security dataset (IoT-Flock)	GNN-BiLSTM (Graph Neural Network + Bidirectional Long Short-Term Memory)	Challenges related to dataset imbalance, real-time detection in resource-constrained environments, and adversarial manipulation of models	Hybrid GNN-BiLSTM model excels in both network traffic data analysis and sequential anomaly detection	99.98%
Okpu et al. (2024)	ToN_IoT Dataset	Feedforward Neural Networks (FNN) and Fuzzy Logic Systems	The system still faces challenges with dataset imbalance, real-time detection in IoMT environments	Hybrid FNN + Fuzzy Logic reduces false alarm rate and improves attack classification in IoMT	99.2%, 0.008% false alarm rate
Alzubi et al. (2024)	CSE-CIC-IDS 2018 Dataset	Blended CNN-LSTM (Convolutional Neural Network + Long Short-Term Memory)	Limited to edge-centric IoMT; computational complexity in handling large-scale attacks.	Combines CNN and LSTM to detect both known and unknown attacks in real-time with high efficiency	98.53%
Fadhil et al. (2024)	WUSTL-EHMS 2020, NSL-KDD Dataset	Hybrid CNN-LSTM (Convolutional Neural Network + Long Short-Term Memory) with	Issues with false positives, hyperparameter tuning, and the	Hybrid Lion Optimization Feature Selection (LOFS) and Grey Wolf	99.26%

		LOFS and GWO optimization	dimensionality of features	Optimizer (GWO) optimize feature selection and hyperparameters, enhancing CNN-LSTM model performance	
Kamil & Mohammed(2023)	UNSW-NB15 Dataset	Hybrid Convolutional Neural Network (CNN) + Dense Layers, Naïve Bayes (NB)	Relies on dataset preprocessing, with potential limitations in performance with complex attacks	The hybrid CNN-Dense model outperforms machine learning models (Naïve Bayes) in both accuracy and detection speed	99.8% accuracy (CNN model) compared to 83% (Naïve Bayes)
Wang et al. (2022)	TADA and TADB IoMT-Blockchain Datasets	Multi-Model Autoencoder (MMAE), BiLSTM, Residual Learning	The model structure is complex and requires multiple pre-training and data conversion steps. It also doesn't cover all possible attack categories in real networks.	The combination of MMAE and BiLSTM enhances feature extraction and classification, with strong anomaly detection performance.	93.5% (TADA), 94.5% (TADB) for multi-class detection

7. Conclusion and Future Work

This study proves the capability of hybrid deep learning models in IoMT-based intrusion detection, and GNN-BiLSTM is the most accurate and generalizable. Results show that IoMT-specific models are far better in detecting malicious activities over other classes and have an accuracy of up to 99.98%. But problems remain, including reducing false positives and tackling real-time considerations such as concurrency for constrained settings.

The study also proposes a few possibilities for future research. The synergy of blockchain and federally based learning has great potential for enhancing security and privacy in IoMT systems. Such developments would provide stronger decentralization of protection and authenticating data, as well as higher resilience to cyberattacks. Future work might focus on

improving the effectiveness and scalability of the models, e.g., to be used in real-time applications.

As a result of the high-performance characteristics, deploying models such as GNN-BiLSTM in hospitals could decrease attack response time by 60%, making security mechanisms more effective for vital healthcare environments. The PS-NG framework is preferred in clear conditions. Furthermore, the GNN-BiLSTM is suitable for high-security areas due to its better performance in a complex environment. They cover all security layers of the IoMT domain.

The overall contribution of this study is that it provides significant insight into the designs of effective IDSs in IoMT. This is just the beginning of advancements in healthcare cybersecurity. A strong partnership between academia, doctors, and cyber experts is required to develop more secure, effective, and resilient systems that protect the privacy of medical data and patient safety in this emerging digital healthcare landscape.

References

Abdualrahman, A. A., & Ibrahem, M. K. (2021). Intrusion detection system using data stream classification. *Iraqi Journal of Science,* 319–328.

Akar, G., Sahmoud, S., Onat, M., Cavusoglu, Ü., & Malondo, E. (2025). L2D2: A Novel LSTM Model for Multi-Class Intrusion Detection Systems in the Era of IoMT. *IEEE Access, 13*, 7002–7013. https://doi.org/10.1109/ACCESS.2025.3526883

Alalhareth, M., & Hong, S.-C. (2023). An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning. *Sensors, 23*(22), 9247. https://doi.org/10.3390/s23229247

Alalhareth, M., & Hong, S.-C. (2024). Enhancing the Internet of Medical Things (IoMT) Security with Meta-Learning: A Performance-Driven Approach for Ensemble Intrusion Detection Systems. *Sensors, 24*(11), 3519. https://doi.org/10.3390/s24113519

Alanazi, H. K., Abd El-Aziz, A. A., & Hamdi, H. (2023). Securing IoT Devices in e-Health using Machine Learning Techniques. *International Journal of Advanced Computer Science and Applications, 14*(9). https://doi.org/10.14569/IJACSA.2023.0140967

Alhijaj, T. B., Hameed, S. M., & Bara'a, A. A. (2021). A decision tree-aware genetic algorithm for botnet detection. *Iraqi Journal of Science,* 2454–2462.

Alzubi, J. A., Alzubi, O. A., Qiqieh, I., & Singh, A. (2024). A blended deep learning intrusion detection framework for consumable edge-centric IoMT industry. *IEEE Transactions on Consumer Electronics, 70*(1), 2049-2057. https://doi.org/10.1109/TCE.2024.3350231

Awotunde, J. B., Abiodun, K. M., Adeniyi, E. A., Folorunso, S. O., & Jimoh, R. G. (2021). A deep learning-based intrusion detection technique for a secured IoMT system. In *International Conference on Informatics and Intelligent Applications* (pp. 50-62). Cham: Springer International Publishing.

Barnawi, A., Chhikara, P., Tekchandani, R., Kumar, N., & Alzahrani, B. (2024). A Differentially Privacy Assisted Federated Learning Scheme to Preserve Data Privacy for IoMT Applications. *IEEE Transactions on Network and Service Management, 21*(4), 4686–4700. https://doi.org/10.1109/TNSM.2024.3393969

Berguiga, A., Harchay, A., & Massaoudi, A. (2025). HIDS-IoMT: A deep learning-based intelligent intrusion detection system for the Internet of Medical Things. *IEEE Access, 13*, 32863–32882. https://doi.org/10.1109/ACCESS.2025.3543127

Dadkhah, S., Neto, E. C. P., Ferreira, R., Molokwu, R. C., Sadeghi, S., & Ghorbani, A. A. (2024). CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT. *Internet of Things, 28*, 101351. https://doi.org/10.1016/j.iot.2024.101351

Daher, L. A. (2023). Towards Secure IoMT: Attack Detection Using Deep Q-Learning in Healthcare Networks. *2023 16th International Conference on Developments in E-Systems Engineering (DeSE)*, 407–412. https://doi.org/10.1109/DeSE58530.2023.00076

Fadhil, H. M., Dawood, Z. O., & Al Mhdawi, A. (2024). Enhancing Intrusion Detection Systems Using Metaheuristic Algorithms. *Diyala Journal of Engineering Sciences,* 15–31.

Fouda, M., Ksantini, R., & Elmedany, W. (2022). A novel intrusion detection system for internet of healthcare things based on deep subclasses dispersion information. *IEEE Internet of Things Journal, 10*(10), 8395–8407.

Gatea, M. J., & Hameed, S. M. (2022). An Internet of Things Botnet Detection Model Using Regression Analysis and Linear Discrimination Analysis. *Iraqi Journal of Science,* 4534–4546.

Judith, A., Kathrine, G. J. W., Silas, S., & J, A. (2023). Efficient Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Devices. *Engineering Proceedings, 59*(1). https://doi.org/10.3390/engproc2023059139

Kamil, W. F., & Mohammed, I. J. (2023). Adapted CNN-SMOTE-BGMM deep learning framework for network intrusion detection using unbalanced dataset. *Iraqi Journal of Science,* 4846–4864.

Kamil, W. F., & Mohammed, I. J. (2023). Deep learning model for intrusion detection system utilizing convolution neural network. *Open Engineering, 13*(1), 20220403. https://doi.org/10.1515/eng-2022-0403

Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access, 8*, 77396–77404. https://doi.org/10.1109/ACCESS.2020.2988955

Memon, S. A., Wiil, U. K., & Shaikh, M. (2023). Explainable Intrusion Detection for Internet of Medical Things. *IC3K - Proceedings, 3*, 40–51. https://doi.org/10.5220/0012210300003598

Mpembele, A. B. (2024). *Differential Privacy-Enabled Federated Learning for 5G-Edge-Cloud Framework in Smart Healthcare*. Tennessee State University.

Nakıp, M., & Gelenbe, E. (2024). Online self-supervised deep learning for intrusion detection systems. *IEEE Transactions on Information Forensics and Security, 19*, 5668-5683. https://doi.org/10.1109/TIFS.2024.3402148

Oh, M.-J., Danuor, P., & Jung, Y.-B. (2023). A study on the optimal magnetic beam forming of coil arrays for long distance wireless power transmission. *Sensors, 23*(11), 5312. https://doi.org/10.3390/s23115312

Okpu, E. O., Taylor, O. E., Nwiabu, N. D., & Matthias, D. (2024). A Hybrid Machine Learning Approach for Intrusion Detection and Mitigation on IoT Smart Healthcare. *International Journal, 13*(7). https://doi.org/10.30534/ijacst/2024/021372024

Park, J., Park, S., Kang, B. B., & Kim, K. (2019). eMotion: An SGX extension for migrating enclaves. *Computers & Security, 80*, 173–185. https://doi.org/10.1016/j.cose.2018.10.019

Ramya, R., Hussein, A. H. A., Adnan, M. M., Shilpa, N., & Priya, S. (2023). Intrusion Detection in Healthcare using Sand-Cat Optimization based Long-Short Term Memory. *2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, 1–5.

Ravi, V., Pham, T. D., & Alazab, M. (2023). Deep learning-based network intrusion detection system for Internet of medical things. *IEEE Internet of Things Magazine, 6*(2), 50–54. https://doi.org/10.1109/IOTM.0001.2300049

Razzaq, R. H., Al-Zubaidie, M., & Atiyah, R. G. (2024). Intermediary Decentralized Computing and Private Blockchain Mechanisms for Privacy Preservation in the Internet of Medical Things. *Mesopotamian Journal of CyberSecurity, 4*(3), 152–165.

Rbah, Y., Mahfoudi, M., Balboul, Y., Chetioui, K., Fattah, M., Mazer, S., Elbekkali, M., & Bernoussi, B. (2023). A Fog-Based Attack Detection Model Using Deep Learning for the Internet of Medical Things. *AISE Proceedings,* 506–511.

Rbah, Y., Mahfoudi, M., Fattah, M., Balboul, Y., Chetioui, K., Mazer, S., Elbekkali, M., & Bernoussi, B. (2024). Hybrid software defined network-based deep learning framework for enhancing internet of medical things cybersecurity. *International Journal of Artificial Intelligence, 13*(3), 3599–3610.

Rbah, Y., Mahfoudi, M., Fattah, M., Balboul, Y., Mazer, S., Elbekkali, M., & Bernoussi, B. (2024). Deep Learning for Enhanced IoMT Security: A GNN-BiLSTM Intrusion Detection System. *2024 International Conference on Circuit, Systems and Communication (ICCSC)*, 1–6.

Revathi, T., Anbazhagan, K., & Kavitha, R. (2024). Utilizing Deep Learning to Enhanced Security in the Internet of Medical Things via Intrusion Detection Systems. *2024 International*

Conference on Emerging Technologies in Computer Science for Interdisciplinary Applications (ICETCS), 1–6.

Saran, N., & Kesswani, N. (2025). Intrusion detection system for the Internet of Medical Things using GRU with attention mechanism–based hybrid deep learning. *Jordanian Journal of Computers and Information Technology, 11*(2). https://doi.org/10.5455/jjcit.71-1725609265

Shambharkar, P. G., & Sharma, N. (2023). Artificial Intelligence Driven Intrusion Detection Framework for the Internet of Medical Things. *Research Square*. https://doi.org/10.21203/rs.3.rs-2634004/v1

Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. (2023). Survey of Machine Learning based intrusion detection methods for Internet of Medical Things. *Applied Soft Computing, 140*, 110227. https://doi.org/10.1016/j.asoc.2023.110227

Sulaiman, S. S., Nadher, I., & Hameed, S. M. (2024). Credit Card Fraud Detection Using Improved Deep Learning Models. *Computers, Materials & Continua, 78*(1), 1049-1069. https://doi.org/10.32604/cmc.2023.046051

Tsimenidis, S., Lagkas, T., & Rantos, K. (2022). Deep learning in IoT intrusion detection. *Journal of Network and Systems Management, 30*(1), 8. https://doi.org/10.1007/s10922-021-09685-y

Vaisakhkrishnan, K., Ashok, G., Mishra, P., & Kumar, T. G. (2024). Guarding Digital Health: Deep Learning for Attack Detection in Medical IoT. *Procedia Computer Science, 235*, 2498–2507. https://doi.org/10.1016/j.procs.2024.01.286

Vijayakumar, K. P., Pradeep, K., Balasundaram, A., & Prusty, M. R. (2023). Enhanced cyber attack detection process for internet of health things (IoHT) devices using deep neural network. *Processes, 11*(4), 1072. https://doi.org/10.3390/pr11041072

Wang, J., Jin, H., Chen, J., Tan, J., & Zhong, K. (2022). Anomaly detection in Internet of medical Things with Blockchain from the perspective of deep neural network. *Information Sciences, 617*, 133–149. https://doi.org/10.1016/j.ins.2022.12.056

Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Communications Surveys & Tutorials, 21*(4), 3723–3768. https://doi.org/10.1109/COMST.2019.2914094