ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 4 (2024)
https://doi.org/ 10.62019/abbdm.v4i4.247

Deep Learning Based Attack Classification on IoMT Devices

Muhammad Awais, Tajummul Hussain, Tayyab Rehman

Chronicle

Article history
Received: November 30, 2024
Received in the revised format: December 18, 2024
Accepted: December 18, 2024
Available online: December 18, 2024

Muhammad Awais is currently affiliated with Institute of Avionics and Aeronautics (IAA) Engineering, Air University Islamabad, Pakistan.
Email: 230332@students.au.edu.pk
Tajummul Hussain is currently affiliated with Department of Electrical Engineering, SS-CASE-IT, Islamabad, Pakistan
Email:engr.tajummalhussain@gmail.com
Tayyab Rehman is currently affiliated with Department of Information Engineering, Computer Science, and Mathematics, University of L'Aquila, Piazza del Santuario, 19, L'Aquila, Italy.
Email:tayyab.rehman@graduate.univaq.it

Abstract

This study gives an in-depth evaluation of deep learning algorithms for threat classifying in the Internet of Medical Things, or IoMT, devices, a rapidly expanding subset of the Internet of Things (IoT) essential for modern healthcare systems. IoMT devices are more susceptible to cyberattacks as they gather, send, and process sensitive medical data, endangering patient security and privacy. Due to particular limitations like low processing power and strong privacy regulations, traditional security solutions usually need to catch up in IoMT circumstances. Consequently, deep learning algorithms offer viable substitutes for real-time, adaptive attack classification due to their capacity to identify intricate patterns in big datasets. Our evaluation and classification of state-of-the-art deep learning algorithms for IoMT security focuses on classification accuracy, computational efficiency, and threat adaption. We discuss significant challenges and opportunities, compare strategies, and assess success metrics. We examine CNNs, RNNs, and hybrid architectures, highlighting how well they can withstand various assaults. This survey will be a thorough resource to direct future studies and advancements in deep learning-based IoMT security

Keywords: Post-Quantum Cryptography (PQC), Quantum Computing Threats, Blockchain Scalability, Quantum Cryptanalysis.

INTRODUCTION

The interconnected system of medical equipment, healthcare IT, and software programs known as the Internet of Medical Things (IoMT) aims to raise the standard, effectiveness, and accessibility of healthcare services (Abbas et al., 2023). The security of these devices has grown essential as healthcare systems depend increasingly on IoMT for real-time monitoring, diagnosis, and therapy management. IoMT devices are particularly vulnerable to cyberattacks since they gather, send, and process many private data, including health information (Mathkor et al.,2024). Additionally, these gadgets are essential to vital healthcare processes, so even minor interruptions can significantly affect patient outcomes. By offering automated, responsive care, this technology is crucial to managing chronic illnesses (Anusha et al., 2024). For example, pacemakers can adapt to abnormal heartbeats by electrically adjusting to preserve normal function. Insulin pumps inside IoMT networks can autonomously deliver doses to control blood glucose levels, which is crucial for managing diabetes (Belkacem et al., 2023). IoMT also includes devices like deep brain implants (DBIs), which use targeted brain stimulation to treat neurological conditions like Parkinson's disease. Besides customized therapies, IoMT applications facilitate more general health requirements, such as fall detection for senior citizens, athlete performance monitoring, and remote patient care for patients in remote locations with inadequate

medical facilities (Li et al., 2023). In addition to improving treatment options, the IoMT produces accurate and comprehensive medical data that improves care efficiency, lowers errors, and makes early disease identification possible. In addition to improving patient outcomes, this move from reactive to preventive healthcare streamlines resources for families, insurance companies, and healthcare providers (Feldman et al., 2023). Patients can now receive care in their homes and avoid frequent hospital visits thanks to the ability to monitor health metrics remotely.

IoMT has the potential to transform the healthcare industry completely. Yet, severe security and privacy concerns exist because it relies on wireless communication routes (Javid et al., 2023). Transmitting private patient information across these networks leaves IoMT devices vulnerable to cyberattacks, which may jeopardize data availability, confidentiality, and integrity. Even essential medical devices like implanted cardioverter-defibrillators, DBIs, and insulin pumps have been hacked recently. This shows that attackers can mess with device operation by getting into these networks without permission (Strik et al., 2023). As the IoMT grows, protecting private and sensitive patient data is crucial to avoiding abuse and preserving patient safety. Maintaining the trust and safety required for IoMT to flourish in contemporary healthcare necessitates overcoming certain obstacles, such as the variety of device types, processing power limitations, and the requirement for low-latency data processing (Bhushan et al., 2023).

Figure 1 depicts the interconnected structure of an Internet of Medical Things (IoMT) ecosystem, where a centralized cloud server connects to various healthcare organizations, including physicians, patients (savvy users), intelligent buildings, smart hospitals, and clever towns. Secure gateways allow each entity to communicate, facilitating device coordination and data transfer across various contexts. Through the cloud server, physicians, medical facilities, and users can see and exchange patient data in real-time, guaranteeing that vital medical information is available for prompt medical interventions and effective healthcare administration. By facilitating smooth integration and connectivity within intelligent healthcare infrastructure, this design improves data accessibility, remote patient care, and coordinated healthcare services in urban environments.

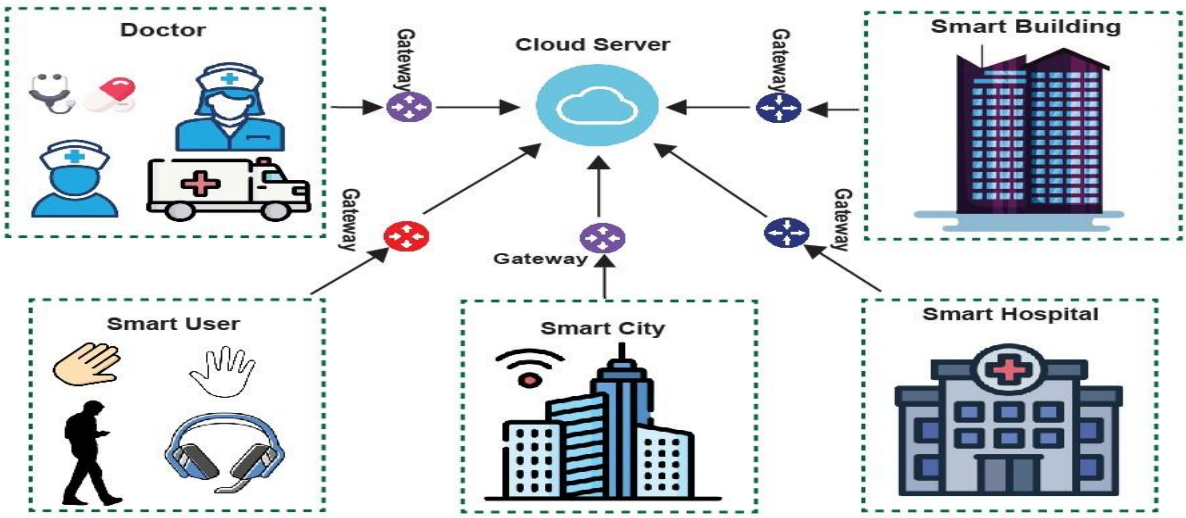

Figure 1:
IoMT Ecosystem Architecture and Connectivity

Strong and flexible security solutions are more critical than ever because of the ongoing increase in cyberattacks that target IoMT. However, standard security measures, such as rule-based systems, signature-based detection, and typical machine learning techniques, often fail to address IoMT-specific issues adequately (Tariq et al., 2023). This is because of things like:

Limited Computational Resources: IoMT devices often have constrained processing power, memory, and storage, making it difficult to deploy complex security solutions (Xie et al. 2024).

Real-Time Processing Needs: Many IoMT applications require low latency to ensure timely medical responses, making it impractical to rely on time-intensive security checks (Diraco et al., 2023).

Privacy Concerns: As IoMT devices handle susceptible data, solutions must also prioritize privacy and ensure patient data is protected throughout the detection process (Zhao et al., 2023).

Real-time cyberattack detection and classification has found a viable solution in deep learning. In contrast to conventional techniques, deep learning models can recognize intricate patterns in vast datasets on their own, allowing them to adjust to different kinds of attacks and react to new dangers (Ajala et al., 2024). Neural networks, for instance, can examine network traffic data from Internet of Medical Things (IoMT) devices to find unusual patterns that could point to an ongoing attack. Figure 2 depicts a multi-layer Internet of Medical Things (IoMT) architecture intended to effectively and securely gather, analyze, and send patient health data. The data gathering layer uses low-power wireless technologies like NFC and BLE to collect health indicators from medical devices, including wearable and stationary equipment, and monitor them continuously.

The Personal Server Layer receives this data and relays it to personal devices, such as smartphones or tablets, which then communicate with gateways (like home Wi-Fi) to transfer information over greater distances via protocols like GSM or Wi-Fi. Healthcare providers can access the centralized servers where the Medical Server Layer processes and archives the data. Medical personnel and monitoring systems use the data at this layer to make decisions and provide real-time patient care. This tiered structure facilitates remote monitoring and prompt interventions by guaranteeing a safe and efficient data transfer from patients to healthcare practitioners.

IoMT device attack classification is intrinsically complicated. Numerous attack types, including ransomware, malware insertion, data spoofing, and denial of service (DoS), have distinct behavioral characteristics. In order to apply the proper countermeasures, security models must be able to precisely identify attacks in addition to detecting them. For example, various mitigating techniques may result from categorizing an attack as a DoS attack vs a data spoofing incident. Attack classification is a mathematically framed multi-class classification task in which we aim to maximize the accuracy of labeling each input data point x. The objective is to identify a function f that minimizes the error rate given a dataset $D = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$, where each x_i is a feature vector taken from network traffic data and y_i is the associated label for the attack type:

$$\min_f \frac{1}{n} \sum_{i=1}^{n} \mathbb{I}(f(x_i) \neq y_i \quad) \qquad (1)$$

where I is the indicator function that assigns a penalty of 1 if the predicted label does not match the actual label and 0 otherwise. Given the variability in attack patterns, a simple linear classification model may struggle to accurately classify attacks. Instead, deep learning models, which can approximate complex non-linear functions, are better suited for this problem.

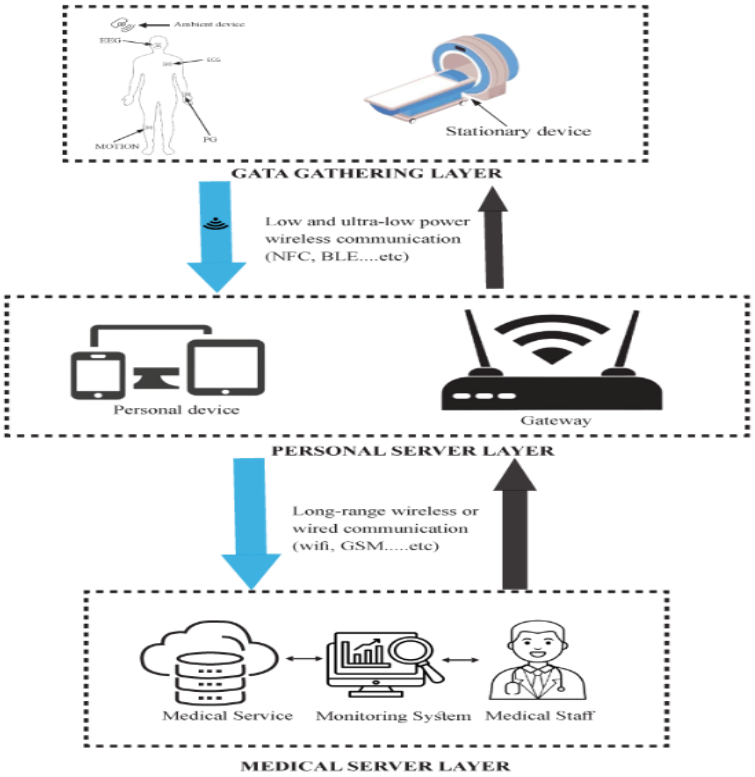

Figure 2:
A layered IoMT system architecture.

Deep Learning Techniques for Attack Classification

Deep learning encompasses a range of models, each with unique advantages for attack classification:

Convolutional Neural Networks (CNNs)

CNNs have traditionally been applied to image processing tasks, but their capacity for spatial feature extraction makes them valuable for identifying patterns in network traffic data. In the context of IoMT, CNNs can process matrix-structured data, such as time-series measurements from medical devices, to identify anomalous patterns that may signify an attack (Brahmi et al., 2024). A CNN layer applies convolution operations, mathematically represented as:

$$h_{i,j}^{l+1} = \sigma\left(\sum_{m,n} w_{m,n}^{l} \cdot h_{(i+m),(j+n)}^{l} + b^{l}\right)$$

where $h_{i,j}^{l+1}$ is the activation in the next layer, $w_{m,n}{}^{l}$ denotes the filter weight at layer l, b^{l} is the bias term, and σ is the activation function. CNNs are highly effective at detecting spatial hierarchies in input data, making them suitable for feature extraction in attack detection (Sarswat et al., 2024).

Recurrent Neural Networks (RNNs)

RNNs, including Long Short-Term Memory (LSTM) networks, are designed to handle sequential data, making them ideal for processing time-dependent logs from IoMT devices. For example, an RNN can analyze the sequence of device operations or network requests to detect unusual behaviors over time (Das et al., 2023). An RNN's recursive structure is formulated as follows: $h_t = \sigma(W_{hh}h_{t-1} + W_{xh}x_t + b)$ (3)

Here, h_t represents the hidden state at time t, x_t is the input at t, W_{hh} and W_{xh} are weight matrices, and b is the bias. LSTMs enhance RNNs with memory cells that retain information over longer sequences, crucial for recognizing extended attack behaviors (Xin et al., 2023).

Hybrid Models

Hybrid models combine CNNs for feature extraction and RNNs for sequence processing, thereby leveraging the strengths of both. Hybrid architectures have demonstrated high accuracy in various cybersecurity applications and are promising for IoMT, where both spatial and temporal features are present (Babu et al., 2024). Each model type has strengths and limitations. CNNs excel at identifying spatial patterns but may overlook temporal relationships, while RNNs are adept at analyzing sequences but may struggle with high-dimensional input. Hybrid models address these limitations by combining both approaches, yet they also increase computational complexity, which may be impractical for some IoMT applications.

Research Objectives and Contributions

The primary objective of this survey is to provide a detailed, research-driven review of deep learning models applied to attack classification in IoMT devices, analyzing each approach's effectiveness, limitations, and adaptability to real-world healthcare applications.

Research Objectives

To Review: Compile and categorize current deep learning methods used in IoMT security, focusing on attack classification performance.

To Compare: Benchmark different deep learning architectures in terms of classification accuracy, processing time, memory requirements, and adaptability to IoMT constraints.

To Identify Gaps: Recognize areas where current approaches may fall short, emphasizing the need for lightweight, privacy-preserving solutions.

Contributions of This Paper

Comprehensive Review: By surveying recent advancements, this paper will offer researchers an extensive resource for understanding the application of deep learning in IoMT attack classification.

Performance Benchmarking: This paper provides a comparative analysis of deep learning models, considering various metrics to aid in the selection of appropriate techniques.

Future Directions: Recommendations for advancing deep learning-based IoMT security, including techniques like federated learning, which distributes training across multiple devices to improve privacy and reduce computational demands.

LITERATURE REVIEW

This study (Shaikh et al., 2024) presents RCLNet, a sophisticated anomaly-based intrusion detection system intended to protect Internet of Medical Things (IoMT) applications, particularly those used in hospital environments. In order to evaluate network traffic and capture spatial and temporal aspects of IoMT data, the RCLNet model uses a hybrid technique that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) models. The study incorporates a preprocessing stage that uses the Random Forest algorithm for feature selection to optimize input data processing. Concentrating on the most pertinent features improves detection efficiency. RCLNet demonstrated its efficacy in detecting known and unknown risks in IoMT systems with an impressive accuracy rate of 99.78% when tested on the WUSTL-EHMS-2020 healthcare dataset. This study shows how RCLNet may significantly increase IoMT security. However, it also stresses the importance of developing the model for effective real-time operation in resource-constrained contexts. In the ever-changing IoMT ecosystem, this study offers a potential path for developing robust and flexible security methods.

The study (Jony et al., 2024) investigated using Long Short-Term Memory (LSTM) networks, a perfect remedy for time-dependent threats, to identify IoMT attacks that display sequential patterns. Their LSTM model improved the system's capacity to recognize prolonged attack behaviors, including ransomware attacks, by analyzing device activity logs to find anomalies over time. A disadvantage of the LSTM network is its high memory and processing requirements despite its strong detection rates on synthetic IoMT datasets. This study emphasizes the trade-off between computational viability and detection accuracy, particularly in IoMT contexts with constrained resources. Future research should investigate hybrid techniques or lighter LSTM variations to preserve good detection accuracy while lowering the computing load.

(Banerjee et al ., 2019) By using CNNs to process geographical information and RNNs to process sequential data, the CNN-RNN model demonstrated exemplary performance in identifying intricate, multi-class assault patterns . When tested on benchmark IoT datasets, the model outperformed solo CNN or RNN models in accuracy. This combination strategy, however, limits its application on real-time IoMT systems with limited processing power because it necessitates more excellent computational resources. The authors suggest further refining the hybrid model or investigating additional effective options to strike a compromise between accuracy and computational viability.

(Samuel Omaji et al., 2023) examined federated learning as a privacy-preserving approach for IoMT security, distributing training across IoMT devices while retaining data locally. Their federated model performed comparably to centralized models in detecting attacks like malware and spoofing but offered enhanced privacy by minimizing data transfer. A challenge identified in the study is the dependence on reliable network connectivity, which may not always be available in IoMT applications. Additionally, the federated structure raises concerns about the model's security, as it could be vulnerable to adversarial attacks. This study suggests improvements in federated frameworks, particularly focusing on privacy and efficiency.

(Liu et al., 2023) investigated using autoencoders to identify irregularities in IoMT networks, emphasizing situations in which labeled data is limited. After learning a compact representation of typical traffic, an autoencoder will reconstruct with a more significant error and flag suspicious data when it encounters anomalous data that doesn't fit the learned structure. They demonstrated that reconstruction errors could successfully distinguish malicious and benign traffic through experiments on artificial IoMT datasets. However, the autoencoder model's inability to correctly categorize particular attack types was a significant flaw in IoMT since various threats frequently call for different responses. Furthermore, the model's capacity to generalize to actual circumstances was questioned because it was trained on artificial data. To improve specificity, the authors propose merging autoencoders with different classification techniques. They also advise future research on hybrid models that enhance classification granularity while maintaining anomaly detection capabilities.

(Khan et al.,2023) used transfer learning to recycle information from previously trained models. To lower the data needs while maintaining accuracy, they built a model on a vast, general IoT dataset before refining it on a smaller, IoMT-specific dataset. According to their findings, transfer learning successfully increased the detection rates of DoS, spoofing, and ransomware attacks. Overfitting issues surfaced, mainly when the source and target dataset differed significantly despite the model's shortened training duration and capacity to adjust to IoMT-specific trends. In practical applications, the overfitting diminished the model's capacity to generalize. This study highlights the need for fine-tuning procedures unique to IoMT contexts and the possibility of transfer learning as a helpful technique in data-limited IoMT scenarios. The authors support further research into creating transfer learning frameworks and IoMT-specific datasets that can reduce overfitting.

(Nuruzzaman Faruqui et al., 2023) propsoed a novel IoMT Intrusion Detection System Using CNN-LSTM Hybridization." This study presents an intrusion detection system (IDS) that integrates convolutional neural networks (CNN) and long short-term memory (LSTM) networks to improve security in the Internet of Medical Things (IoMT). SafetyMed is a suggested system that can identify intrusions from sequential and gridstructured data with an average accuracy of 97.63%. The article also discusses issues with IoMT devices' computational constraints. It offers optimization techniques to balance false positives and detection rates.

The paper (Zhang et al., 2019) addresses issues in natural language processing by investigating the use of Capsule Networks (CapsNets) to extract many relations from a single utterance. The authors suggest an attentive capsule network that efficiently captures hierarchical properties to improve the model's capacity to recognize complex relationships. However, they also acknowledge that CapsNets' high processing overhead may be a drawback for real-time applications. The paper recommends more excellent investigation into optimizing CapsNet topologies to lower computing demands and increase their suitability for contexts with limited resources and time.

(Francisco S. Mel´ıcias et.al.,2024) concentrated on employing data augmentation methods to increase the resilience of threat categorization models on the Internet of Medical Things (IoMT). To enhance model generalization across different attack types, especially in data-limited circumstances, they used techniques including random sampling, rotation, and synthetic sample production to enrich IoMT datasets. Although

they warned that incorrect implementation would introduce noise, thereby diminishing reliability and skewing results, their studies showed that data augmentation could significantly improve model performance. To preserve model fidelity, the authors underlined the significance of adjusting augmentation techniques to correspond with actual attack circumstances. The table 1. provides an overview of current IoMT security methods, emphasizing significant developments in anomaly detection and data augmentation while tackling issues with computational limitations and the viability of real-time applications.

Table 1.
Literature Review Summary

Study	Focus	Techniques	Findings	Limitations
Shaikh et al. (2024)	RCLNet for anomaly-based intrusion detection in IoMT	CNN, LSTM, Random Forest for feature selection	Achieved 99.78% accuracy on WUSTLEHMS-2020 dataset	High resource requirement for real-time IoMT applications
Jony et al. (2024)	LSTM for sequential pattern recognition in IoMT attacks	Long Short-Term Memory (LSTM)	Improved detection of ransomware over time	High memory and processing needs
Banerjee et al. (2019)	CNN-RNN for multi-class IoT attack detection	Combination of CNN and RNN	Outperformed single CNN/RNN models on IoT datasets	High computational demand for real-time systems
Omaji et al. (2022)	Federated learning for privacy in IoMT security	Federated learning across devices	Maintained privacy, but vulnerable to adversarial attacks	Reliant on network connectivity and adversarial threats
Liu et al. (2023)	Autoencoders for anomaly detection with limited labeled data	Autoencoder reconstruction errors	Effective distinction of malicious/benign traffic	Limited attack categorization and generalization
Khan et al. (2023)	Transfer learning for improved IoMT attack detection	Transfer learning from IoT to IoMT datasets	Higher detection rates but risk of overfitting	Overfitting when datasets differ
Faruqui et al. (2023)	SafetyMed IDS using CNN-LSTM hybridization	CNN and LSTM integration	97.63% accuracy in intrusion detection	Computational constraints on IoMT devices
Zhang et al. (2019)	Capsule Networks for relation extraction in NLP	Capsule Networks (CapsNets)	Captured complex relations but high computational load	CapsNets demand high processing power
Mel´ıcias et al. (2024)	Data augmentation to enhance IoMT threat classification	Data augmentation (sampling, rotation, synthetic data)	Improved generalization but risk of noise if misused	Risk of noise affecting accuracy

Current Techniques in Deep Learning for IoMT Security

Since the Internet of Medical Things (IoMT) devices manage susceptible patient data and manage vital healthcare systems, their security is crucial. Deep learning has been a potent instrument for IoMT security in recent years, providing pattern recognition-based threat detection and classification techniques. Examining the leading deep learning models Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long

Short-Term Memory (LSTM) networks, and hybrid architectures—this section also looks at new approaches that tackle IoMT-specific problems, such as federated learning, differential privacy, and reinforcement learning. There is also a discussion of the evaluation metrics used to compare these models.

Deep Learning Models

Convolutional Neural Networks (CNNs): Originally created for image recognition, Convolutional Neural Networks (CNNs) are a class of deep learning models that use convolutional and pooling layers to exploit spatial hierarchies in data. IoMT uses CNNs to analyze structured data, including network traffic logs and time-series health measures (Salehi et al. 2023). In order to find features like anomalous access patterns, network invasions, or unauthorized device interactions, CNNs' convolutional layers employ tiny filters to search data for local patterns. A CNN's primary function is convolution, which creates feature maps by applying a filter *w* across tiny areas of the input matrix *X*. The output feature map $h_{i,j}^{(l+1)}$ at position (*i,j*) for each layer *l* is described mathematically as follows:

$$h_{i,j}^{(l+1)} = \sigma\left(\sum_{m,n} w_{m,n}^{(l)} \cdot h_{(i+m),(j+n)}^{(l)} + b^{(l)}\right)$$

where $w_{m,n}^{(l)}$ is the filter at layer l, $h_{i,j}^{(l)}$ is the input at layer *l*, $b^{(l)}$ is the bias, and σ is an activation function, which is frequently the ReLU function $\sigma(x) = \max(0,x)$. CNNs are skilled at identifying patterns in the structured input data frequently encountered in IoMT applications because they are able to capture hierarchical spatial information by stacking multiple convolutional and pooling layers (Ahad et al., 2023). CNNs are excellent at identifying spatial patterns, but they are unable to identify sequential dependencies, which are crucial in attacks that change over time. On IoMT networks, this restriction frequently results in less-than-ideal performance when it comes to identifying sophisticated attack activities like advanced persistent threats (APTs) (Arslan et al. 2024). Hybrid architectures sometimes mix CNNs with temporal models for improved performance.

Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) Networks

Recurrent neural networks (RNNs) are a good fit for evaluating time-dependent logs in IoMT, where patterns emerge over time because they are naturally good at processing sequential data . RNNs may identify temporal dependencies in sequential data, such as a device's access history or network traffic patterns, using recursive hidden states to store information from prior inputs. A typical RNN updates its hidden state h_t in this way:

$$ht = \sigma(Whhht-1 + Wxhxt + b)$$

where W_{hh} and W_{xh} are weight matrices, x_t is the input at time *t*, and *b* is the bias. However, vanishing gradients cause problems for RNNs with long-term dependencies, which restricts their capacity to recognize patterns in long sequences (Ghojogh et al., 2023). The introduction of Long Short-Term Memory (LSTM) networks circumvented these constraints. Long-term memory cells, controlled by input, forget, and output gates, are a component of LSTMs. It is these gates that update the cell state C_t:

$$Ct = ft \cdot Ct-1 + it \cdot C\tilde{}t$$

where $\tilde{C}_t$ denotes the candidate cell state and f_t, i_t, and o_t are the forget, input, and output gates, respectively. LSTMs are more suitable for IoMT applications where attack patterns may emerge gradually or over many transactions since they preserve information over extended sequences (Durstewitz et al., 2023, Shiri et al., 2023). Despite their benefits, LSTMs' computational demands can challenge IoMT devices with constrained processing power. One possible option is to employ remote server processing or lighter variants of LSTMs, like GRUs (Gated Recurrent Units) (Wan et al., 2023)

Hybrid Architectures

Models can capture spatial and temporal aspects in IoMT attack data thanks to hybrid architectures, which integrate CNNs for spatial pattern identification with LSTMs or RNNs for sequential data processing (Lahmar et al., 2023). These designs are particularly well-suited for intricate IoMT attack scenarios because they usually use CNN layers to extract pertinent spatial features from time-series data, followed by LSTM layers that analyze this information over time. Although hybrid models require improvements for deployment on IoMT devices, they are computationally expensive and successfully increase accuracy in multi-class attack classification tasks (Lieber et al., 2024). Using spatial and temporal analysis, hybrid architectures offer a complete solution for identifying and classifying IoMT hazards, from sudden anomalies to gradually developing threats.

Emerging Techniques

Federated Learning

Federated learning is a decentralized deep learning technique that protects data privacy by enabling IoMT devices to work together to train a model without exchanging raw data. Local data is used by each device to update its model, which is then combined into a global model (Qi et al., 2024). A mathematical calculation of the global model $w^{(t+1)}$ at iteration $t + 1$ is as follows:

$$w^{(t+1)} = \frac{1}{N} \sum_{i=1}^{N} w_i^{(t)}$$

where N is the number of devices and $w_i^{(t)}$ is the model parameters on device i at iteration t. The limited computational capabilities of individual devices make it difficult to ensure model robustness and efficiency. However, federated learning allows IoMT networks to enhance security models while adhering to privacy standards (Beltr´an et al., 2023).

Differential Privacy

By introducing noise into the model or data, differential privacy improves privacy by preventing the extraction of specific data points. The following is satisfied by the differential privacy mechanism:

$$P(f(x) \in S) \leq e^{\epsilon} \times P(f(x') \in S)$$

where ϵ is a privacy-controlling parameter, x and x' are adjacent datasets, and S is the collection of potential outputs. Although the additional noise may affect model accuracy, differential privacy is used in IoMT in combination with deep learning models to protect patient privacy while facilitating precise threat identification (Yang et.al, 2023).

Reinforcement Learning

In IoMT security, reinforcement learning (RL) makes adaptive response systems possible by teaching an agent to optimize rewards for precise attack categorization and reaction

(Shakya et al., 2023) . The RL agent uses its environment to optimize its policy for making decisions based on a reward function, which is represented as follows: $Q(s,a) = R(s,a) + \gamma \max_{a'} Q(s,' a')$

Where *R*(*s*,*a*) is the instantaneous reward for action *a*, γ is the discount factor, and *Q*(*s*,*a*) is the quality of action *a* in state *s*. Although reinforcement learning is useful for identifying intricate, dynamic threats in IoMT, it necessitates a large amount of processing power and careful incentive structure adjustment to avoid unintended consequences (Abel et al., 2024) .

Evaluation Metrics: Evaluation metrics are critical for assessing the performance of IoMT security models. Key metrics include:

Accuracy: The ratio of correctly classified cases to total cases, reflecting overall model performance.

Precision: Precision measures the proportion of true positive predictions among all positive predictions:

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives + False Positives}}$$

Recall: Recall calculates the proportion of true positive cases detected out of all actual positive cases:

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives + False Negatives}}$$

F1-score: The harmonic mean of precision and recall, balancing both metrics:

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision + Recall}}$$

Computational Efficiency: This metric evaluates the model's resource requirements, including time complexity and memory usage.

Adaptability: Adaptability measures a model's ability to generalize across various IoMT scenarios, ensuring robustness in real-world applications.

Dataset and Attack Types

Data Sources: The quality and completeness of the training and testing datasets are critical to the efficacy of deep learning models for IoMT security. However, privacy issues, data heterogeneity, and the particular operating environment of medical devices limit the availability of real-world, labeled IoMT datasets. This section covers standard datasets, methods for creating synthetic data, and researchers' difficulties in obtaining accurate IoMT data.

Popular Datasets

NSL-KDD: Since the NSL-KDD dataset has a better distribution than the original KDD'99 dataset, it has been widely used in cybersecurity research (Zakariah et al., 2023). In addition to standard and attack behaviors, such as DoS, R2L (Remote-to-Local), U2R (User-to-Root), and probing assaults, it offers labeled network traffic logs. NSL-KDD is helpful for general network security. However, its direct relevance for IoMT threat detection is limited since it lacks the specificity of IoMT contexts, such as wearable health monitoring or diagnostic device data (Yuliana et al., 2024).

UNSW-NB15: The UNSW-NB15 dataset was developed to represent contemporary network traffic and contains a range of attack types including DoS, backdoors, exploits, fuzzers, and reconnaissance (Vibhute et al., 2024). This dataset offers a broader scope of attacks than NSL-KDD and provides richer feature sets that support advanced intrusion detection studies. However, UNSW-NB15 does not account for IoMT-specific communication protocols or device interactions, requiring adaptation to be fully effective in medical IoT applications (Kumar et al., 2024).

CICIDS2017: The CICIDS2017 dataset is a comprehensive dataset created by the Canadian Institute for Cybersecurity, which includes modern attack types such as botnets, brute-force, and DoS attacks. It provides detailed network traffic flow data, including timestamps, IP addresses, and protocols, supporting deep learning-based security models (Phulre et al., 2023). Although suitable for IoT applications, CICIDS2017 does not contain IoMT-specific device interactions, which means it may not fully capture the complexity of medical device networks.

TON IoT: The TON IoT dataset represents network and telemetry data from IoT devices in smart environments, including data on DDoS, DoS, and reconnaissance attacks. It provides telemetry data that can be useful for anomaly detection in IoMT [48]. Although TON IoT is more relevant for IoT security research, its focus on smart homes and industrial IoT means it lacks the healthcare-specific data necessary for robust IoMT model training.

Synthetic Data Generation Techniques

Due to the scarcity of real IoMT datasets, synthetic data generation has become a valuable tool in IoMT research, allowing for the creation of controlled, varied, and labeled datasets. Recent studies highlight three main synthetic data generation techniques:

Generative Adversarial Networks (GANs): For security applications like IoMT, GANs have produced convincing synthetic data. A GAN configuration uses a generator network to create fake samples and a discriminator network to determine if they are real. GAN-generated synthetic attack traffic has the potential to diversify training data, leading to improved model generalization and detection accuracy. In order to generate data that is useful to IoMT and represents real traffic from healthcare devices, GANs need to be fine-tuned and can be unstable (Abdusalomov et al. 2023).

Data Augmentation: Network data augmentation in IoMT research has evolved from traditional data augmentation methods like scaling values, introducing noise, or altering timestamps. To make models more resistant to overfitting, data augmentation is excellent for growing datasets with little changes to existing records (Garcea et al., 2023). They Discovered that deep learning models had a performance boost of up to 12% from data augmentation when it came to identifying uncommon abnormalities related to IoMT.

Simulation Environments

Researchers can generate realistic attack scenarios by simulating interactions with IoMT devices using tools like CyberRange and IoTIFY. By using simulation environments, researchers can test out complex assaults in a safe environment.

Challenges in Obtaining Realistic IoMT Data

Data Privacy and Compliance: Due to regulatory restrictions such as HIPAA in the U.S. and GDPR in the EU, medical IoT data is subject to strict privacy protections. Researchers face challenges in obtaining large-scale, real-world IoMT datasets that contain patient information.

Device and Network Heterogeneity: IoMT devices vary widely in their functionalities, network protocols, and data formats. This heterogeneity complicates dataset standardization and introduces variability in data quality.

Attack Diversity: The constantly evolving threat landscape necessitates diverse datasets that reflect modern IoMT-specific attacks, such as medical ransomware, data tampering, and device hijacking.

Real-Time Requirements: IoMT devices often operate under strict latency constraints, especially in applications such as real-time patient monitoring.

Types of Attacks in IoMT

IoMT devices are vulnerable to various assault types, each with unique characteristics and consequences for healthcare systems. We delineate principal attack vectors in IoMT contexts, citing conclusions from recent studies. Table 2 delineates various attacks and their consequences.

Denial of Service (DoS) Attacks

A denial-of-service attack (DoS) aims to make a device unavailable to its intended users by flooding it with requests or data. Attacks on the DoS can impede healthcare providers' access to vital data in an IoMT setting, which could postpone patient care it demonstrated that, in simulations, denial-of-service attacks on hospital networks significantly affected healthcare operations by increasing response times by 30% (Ali et al., 2023).

Ransomware

Ransomware attacks aim to encrypt data on devices and then demand payment to unlock it. Because of the critical nature of patient data access, this attack is especially disastrous in the healthcare industry. It has been revealed that ECG monitors and other Internet of Medical Things (IoMT) equipment are vulnerable to ransomware attacks, which, if not paid, might cause diagnostic delays or even data loss (Vistro et al., 2024).

Data Spoofing

Data spoofing entails the fabrication of information conveyed by IoMT devices. Spoofing attacks can deceive healthcare providers, as fabricated health measurements may suggest inaccurate patient conditions. It discovered that falsified data from wearable devices, such as oxygen saturation levels, could result in erroneous treatment if noticed, presenting substantial dangers to patient safety [53].

Malware Injection

Malware injection embeds harmful code into IoMT devices, jeopardizing their functioning, security, or data integrity. Malware may extract sensitive patient information or interfere with device functionality. They demonstrated that malware-infected IoMT devices had a 40% increased incidence of operational failure, indicating significant repercussions for healthcare environments (Zapzalka et al., 2024). In conclusion, the development of effective IoMT security models relies on access to diverse, high-quality datasets that reflect realistic IoMT threats and device interactions. Although publicly available datasets like NSL-KDD and CICIDS2017 offer foundational support, they lack the specificity necessary for IoMT. Synthetic data generation techniques, including GANs, data augmentation, and simulation environments, have become essential tools for enhancing dataset diversity. Understanding the types of attacks that threaten IoMT devices is equally crucial, as different attacks have varied impacts on patient safety and healthcare efficiency.

Table 2:
Types of Attacks in IoMT and their Impact on Healthcare

Attack Type	Description	Example Impact in Healthcare
Denial of Service (DoS)	Overloads resources to make devices or services unavailable	Disrupts patient monitoring in critical care
Ransomware	Encrypts data, demanding ransom for decryption	Blocks access to patient health records, delays treatment
Data Spoofing	Modifies or falsifies transmitted data	Leads to misdiagnosis due to altered telemetry data
Malware Injection	Injects malicious software to compromise devices	Enables data theft, unauthorized access, further attacks

Open Research Challenges

Deploying strong and flexible deep learning-based security models presents several research issues due to the distinct operating environment and crucial significance of Internet of Medical Things (IoMT) devices. Notwithstanding recent developments, current methods' scalability, interpretability, generalizability, and privacy preservation are all constrained. This section looks closely at these issues and identifies possible lines of inquiry for further research.

Scalability

The scalability of networks in IoMT environments is a critical challenge, as they may contain thousands of heterogeneous devices, such as wearables, implantable sensors, and diagnostic equipment. To accommodate the increasing volume of devices and the corresponding data, deep learning models employed in IoMT security must be capable of scaling without sacrificing performance or latency. Substantial computational resources are frequently unavailable in constrained IoMT devices, even though conventional deep learning architectures necessitate them. Furthermore, the resourceintensive character of deep models poses obstacles in real-time applications, where low latency and continuous monitoring are indispensable.

Recent studies have suggested using lightweight models, such as SqueezeNets and MobileNets, to address scalability to address scalability. However, these methods frequently sacrifice accuracy for efficiency, which may be counterproductive in high-stakes healthcare applications. Future research should explore distributed architectures,

including federated learning and edge computing, which facilitate collaborative model training across multiple devices without centralizing data to enable scalable IoMT security. Edge computing can decrease latency by processing data near the source. At the same time, federated learning allows devices to train models locally and share only model updates, thereby preserving privacy and scalability.

Interpretability of Deep Learning Models

The capacity to comprehend and rely on model predictions, or interpretability, is essential in healthcare, as patient outcomes are susceptible to decisions. Healthcare providers frequently encounter difficulties understanding the reasoning behind predictions, as deep learning models, particularly those employed for anomaly detection and classification, are commonly perceived as "black boxes." For example, clinicians may find it challenging to respond to a model that indicates anomalous behavior in an ECG monitor without explaining its decision-making.

To improve the interpretability of models, recent developments in explainable AI (XAI) techniques, including Shapley Additive Explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME), have emerged. Nevertheless, integrating these techniques into real-time IoMT applications presents a challenge. XAI methods can introduce additional computational overhead, impacting scalability and latency. Future research should concentrate on developing interpretability frameworks to optimize efficacy and interpretability in resource-constrained IoMT environments. self-interpretable models are a promising approach, as they incorporate interpretability directly into the model architecture, enabling real-time interpretability without the need for post-hoc analysis.

Generalizability Across IoMT Devices

IoMT devices exhibit significant variability in hardware capabilities, communication protocols, and operating environments, resulting in issues with model generalizability. A model trained on data from a particular type of IoMT device, such as a wearable cardiac monitor, may exhibit suboptimal performance on data from other devices, such as implantable insulin pumps or diagnostic imaging systems. The problem is intensified by disparities in data distributions, device-specific noise, and fluctuations in attack patterns among devices.

Domain adaptation and transfer learning are effective methodologies for improving model generalizability across diverse IoMT devices. Domain adaptation enables models to modify new data distributions by transferring information from a source domain to a target domain. Transfer learning facilitates the application of pre-trained models to analogous tasks, diminishing the requirement for substantial labeled data in the target domain. A recent study by Zhang et al. demonstrated that transfer learning enhanced model performance by up to 15% in cross-device IoMT applications. Nonetheless, domain adaptation and transfer learning methodologies must be tailored to the low-power, real-time requirements of IoMT, prioritizing lightweight architectures and efficient training algorithms.

Privacy-Preserving Techniques

Due to the delicate nature of medical data, privacy is a critical concern in IoMT security. IoMT devices gather and transmit patient data, making them susceptible to privacy

violations that may have significant legal and ethical consequences. Conventional techniques for safeguarding data privacy, such as encryption, can need considerable processing resources, which could be more practical for low-power IoMT devices. Moreover, centralized data storage and processing, prevalent in traditional deep learning frameworks, pose hazards of unwanted access and data exploitation. To tackle these difficulties, researchers are investigating privacy-preserving approaches, like federated learning, differential privacy, and homomorphic encryption. Federated learning enables the training of models using decentralized data, wherein only model updates are communicated while the data remains confidential. This solution mitigates privacy problems but necessitates secure aggregation techniques to avert leakage from model updates.

Differential privacy introduces statistical noise to data or model parameters, guaranteeing that individual data points remain indistinguishable from the model's output. Nonetheless, differential privacy may diminish model accuracy, creating a trade-off between privacy and performance. Homomorphic encryption facilitates computations on encrypted data, permitting IoMT devices to handle sensitive information without decryption. Despite its potential, homomorphic encryption is computationally intensive. It may not be feasible to use real-time Internet of Medical Things applications. Future research should focus on enhancing these techniques for IoMT contexts via hardware acceleration or hybrid methodologies that integrate privacy-preserving strategies with lightweight models.

Future Directions

Addressing these open research challenges requires innovative approaches that extend beyond current methodologies. Below are suggested avenues for future work:

Scalable Federated Learning Frameworks: Develop federated learning frameworks specifically tailored to the scalability and heterogeneity of IoMT devices, incorporating techniques such as hierarchical federated learning and adaptive federated optimization to minimize communication costs and computation.

Real-Time Explainability Models: Investigate real-time self-interpretable models for IoMT, balancing interpretability and computational efficiency. Future models should offer on-device interpretability without the need for resource-intensive post-hoc XAI techniques.

Domain Adaptive Algorithms: Enhance transfer learning and domain adaptation algorithms that can dynamically adjust to IoMT's device-specific variations, incorporating meta-learning techniques to improve adaptability in diverse environments.

Lightweight Privacy Mechanisms: Explore privacy-preserving mechanisms that integrate differential privacy with federated learning, aiming to create adaptive privacy controls that balance security with performance in resource-limited IoMT devices. The research challenges in IoMT security reflect the need for specialized approaches to ensure scalability, interpretability, generalizability, and privacy. Current solutions have demonstrated partial success, but further research is needed to develop models that can operate effectively under IoMT constraints. As IoMT continues to expand, addressing these challenges will be essential for safeguarding patient data and maintaining trust in healthcare technology.

CONCLUSION

This paper examines the pivotal role of deep learning approaches in enhancing the security of Internet of Medical Things (IoMT) systems. The security of IoMT devices is crucial due to their incorporation into healthcare systems and their role in handling sensitive patient data. As IoMT devices grow, the complexity of safeguarding these networks against increasingly sophisticated cyber threats also escalates. Our analysis of contemporary methodologies underscored the efficacy of Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), hybrid architectures, and innovative strategies such as federated learning and differential privacy in tackling the distinct issues associated with the Internet of Medical Things (IoMT). Our review identified several open research challenges, including the scalability of security models for extensive networks of heterogeneous devices, the interpretability of model predictions to facilitate decision-making in clinical settings, the generalizability of solutions across various IoMT devices, and the urgent requirement for privacy-preserving mechanisms designed for the sensitive data landscape of IoMT. Current solutions exhibit considerable progress, yet they must address all IoMT limitations concurrently. Models require further optimization to reconcile accuracy, latency, and privacy demands while functioning within the constrained processing capabilities of IoMT devices.

The results highlight the imperative for ongoing research and innovation in IoMT security. Future research should concentrate on creating scalable, interpretable, and adaptive deep learning models tailored to the restrictions and requirements of medical IoT. Furthermore, progress in privacy-preserving methodologies that align with the real-time requirements of IoMT will be crucial for secure and compliant operations. With the expansion of the IoMT ecosystem, robust and specialized security frameworks will be essential to safeguard patient data, uphold healthcare quality, and enhance trust in linked medical technology. In summary, protecting IoMT settings is both a technical difficulty and a vital healthcare necessity. Addressing the intricacies of IoMT security through continuous research in deep learning solutions will be essential for the future of secure and dependable healthcare systems. This will facilitate the adoption of IoMT while safeguarding patient data and guaranteeing system resilience.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally to the creation of this work.
Conflicts of Interests: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Abbas, T., Khan, A.H., Kanwal, K., Daud, A., Irfan, M., Bukhari, A., Alharbey, R.: Iomt-based healthcare systems: A review. Computer Systems Science & Engineering 48(4) (2024)

Mathkor, D.M., Mathkor, N., Bassfar, Z., Bantun, F., Slama, P., Ahmad, F., Haque, S.: Multirole of the internet of medical things (iomt) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. Journal of infection and public health (2024)

Anusha, V.S., Kumar, R.K., Kumar, G.C., Mabjan, P.: Comprehensive survey on internet of medical things (iomt)-applications and challenges. In: 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1–5 (2024). IEEE

Belkacem, A.N., Jamil, N., Khalid, S., Alnajjar, F.: On closed-loop brain stimulation systems for improving the quality of life of patients with neurological disorders. Frontiers in human neuroscience 17, 1085173 (2023)

Li, Z., Li, H., Meng, L.: Model compression for deep neural networks: A survey. Computers 12(3), 60 (2023)

Riis, T.S., Feldman, D.A., Vonesh, L.C., Brown, J.R., Solzbacher, D., Kubanek, J., Mickey, B.J.: Durable effects of deep brain ultrasonic neuromodulation on major depression: a case report. Journal of Medical Case Reports 17(1), 449 (2023)

Javed, A., Awais, M., Shoaib, M., Khurshid, K.S., Othman, M.: Machine learning and deep learning approaches in iot. PeerJ Computer Science 9, 1204 (2023)

Strik, M., Sacristan, B., Bordachar, P., Duchateau, J., Eschalier, R., Mondoly, P., Laborderie, J., Gassa, N., Zemzemi, N., Laborde, M., *et al.*: Artificial intelligence for detection of ventricular oversensing: Machine learning approaches for noise detection within nonsustained ventricular tachycardia episodes remotely transmitted by pacemakers and implantable cardioverter-defibrillators. Heart Rhythm 20(10), 1378–1384 (2023)

Bhushan, B., Kumar, A., Agarwal, A.K., Kumar, A., Bhattacharya, P., Kumar, A.: Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends. Sustainability 15(7), 6177 (2023)

Tariq, U., Ahmed, I., Khan, M.A., Bashir, A.K.: Fortifying iot against crimpling cyber-attacks: a systematic review. Karbala International Journal of Modern Science 9(4), 9 (2023)

Xie, J., Jia, Q., Chen, Y., Wang, W.: Computation offloading and resource allocation in satellite-terrestrial integrated networks: A deep reinforcement learning approach. IEEE Access (2024)

Diraco, G., Rescio, G., Siciliano, P., Leone, A.: Review on human action recognition in smart living: Sensing technology, multimodality, real-time processing, interoperability, and resource-constrained processing. Sensors 23(11), 5281 (2023)

Zhao, R., Zhang, Y., Zhu, Y., Lan, R., Hua, Z.: Metaverse: Security and privacy concerns. Journal of Metaverse 3(2), 93–99 (2023)

Ajala, O.A., Okoye, C.C., Ofodile, O.C., Arinze, C.A., Daraojimba, O.D., *et al.*: Review of ai and machine learning applications to predict and thwart cyberattacks in real-time. Magna Scientia Advanced Research and Reviews 10(1), 312– 320 (2024)

Brahmi, W., Jdey, I., Drira, F.: Exploring the role of convolutional neural networks (cnn) in dental radiography segmentation: A comprehensive systematic literature review. Engineering Applications of Artificial Intelligence 133, 108510 (2024)

Sarswat, P.K., Singh, R.S., Pathapati, S.V.S.H.: Real time electronic-waste classification algorithms using the computer vision based on convolutional neural network (cnn): Enhanced environmental incentives. Resources, Conservation and Recycling 207, 107651 (2024)

Das, S., Tariq, A., Santos, T., Kantareddy, S.S., Banerjee, I.: Recurrent neural networks (rnns): architectures, training tricks, and introduction to influential research. Machine Learning for Brain Disorders, 117–138 (2023)

Xin, J., Zhou, C., Jiang, Y., Tang, Q., Yang, X., Zhou, J.: A signal recovery method for bridge monitoring system using tvfemd and encoder-decoder aided lstm. Measurement 214, 112797 (2023)

Babu, R.M., Satamraju, K.P., Gangothri, B.N., Malarkodi, B., Suresh, C.V.: A hybrid model using genetic algorithm for energy optimization in heterogeneous internet of blockchain things. Telecommunications and Radio Engineering 83 (2024)

Shaikh, J.A., Wang, C., Muhammad, W.U.S., Arshad, M., Owais, M., Alnashwan, R.O., Chelloug, S.A., Muthanna, M.S.A.: Rclnet: an effective anomaly-based intrusion detection for securing the iomt system. Frontiers in Digital Health 6, 1467241 (2024)

Jony, A.I., Arnob, A.K.B.: A long short-term memory based approach for detecting cyber attacks in iot using cic-iot2023 dataset. Journal of Edge Computing 3(1), 28–42 (2024)

Banerjee, I., Ling, Y., Chen, M.C., Hasan, S.A., Langlotz, C.P., Moradzadeh, N., Chapman, B., Amrhein, T., Mong, D., Rubin, D.L., *et al.*: Comparative effectiveness of convolutional neural network (cnn) and recurrent neural network (rnn) architectures for radiology text report classification. Artificial intelligence in medicine 97, 79–88 (2019)

Samuel, O., Omojo, A.B., Onuja, A.M., Sunday, Y., Tiwari, P., Gupta, D., Hafeez, G., Yahaya, A.S., Fatoba, O.J., Shamshirband, S.: Iomt: A covid-19 healthcare system driven by federated learning and blockchain. IEEE Journal of Biomedical and Health Informatics 27(2), 823–834 (2022)

Liu, Y., Guo, Y., Du, K., Cao, L.: Enhanced memory adversarial network for anomaly detection. In: Chinese Conference on Biometric Recognition, pp. 417–426 (2023). Springer

Khan, T.A., Fatima, A., Shahzad, T., Alissa, K., Ghazal, T.M., Al-Sakhnini, M.M., Abbas, S., Khan, M.A., Ahmed, A., *et al.*: Secure iomt for disease prediction empowered with transfer learning in healthcare 5.0, the concept and case study. IEEE Access 11, 39418–39430 (2023)

Faruqui, N., Yousuf, M.A., Whaiduzzaman, M., Azad, A., Alyami, S.A., Li`o, P., Kabir, M.A., Moni, M.A.: Safetymed: a novel iomt intrusion detection system using cnn-lstm hybridization. Electronics 12(17), 3541 (2023)

Zhang, X., Li, P., Jia, W., Zhao, H.: Multi-labeled relation extraction with attentive capsule network. In: Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, pp. 7484–7491 (2019)

Mel´ıcias, F.S., Ribeiro, T.F., Rabad˜ao, C., Santos, L., Costa, R.L.d.C.: Gpt and interpolation-based data augmentation for multiclass intrusion detection in iiot. IEEE Access (2024)

Salehi, A.W., Khan, S., Gupta, G., Alabduallah, B.I., Almjally, A., Alsolai, H., Siddiqui, T., Mellit, A.: A study of cnn and transfer learning in medical imaging: Advantages, challenges, future scope. Sustainability 15(7), 5930 (2023)

Ahad, M.T., Li, Y., Song, B., Bhuiyan, T.: Comparison of cnn-based deep learning architectures for rice diseases classification. Artificial Intelligence in Agriculture 9, 22–35 (2023)

Arslan, M., Mubeen, M., Bilal, M., Abbasi, S.F.: 1d-cnn-ids: 1d cnn-based intrusion detection system for iiot. arXiv preprint arXiv:2409.08529 (2024)

Ghojogh, B., Ghodsi, A.: Recurrent neural networks and long short-term memory networks: Tutorial and survey. arXiv preprint arXiv:2304.11461 (2023)

Durstewitz, D., Koppe, G., Thurm, M.I.: Reconstructing computational system dynamics from neural data with recurrent neural networks. Nature Reviews Neuroscience 24(11), 693–710 (2023)

Shiri, F.M., Perumal, T., Mustapha, N., Mohamed, R.: A comprehensive overview and comparative analysis on deep learning models: Cnn, rnn, lstm, gru. arXiv preprint arXiv:2305.17473 (2023)

Wan, A., Chang, Q., Khalil, A.-B., He, J.: Short-term power load forecasting for combined heat and power using cnn-lstm enhanced by attention mechanism.

Energy 282, 128274 (2023)

Lahmar, C., Idri, A.: Deep hybrid architectures for diabetic retinopathy classification. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization 11(2), 166–184 (2023)

Lieber, O., Lenz, B., Bata, H., Cohen, G., Osin, J., Dalmedigos, I., Safahi, E., Meirom, S., Belinkov, Y., Shalev-Shwartz, S., et al.: Jamba: A hybrid transformermamba language model. arXiv preprint arXiv:2403.19887 (2024)

Qi, P., Chiaro, D., Guzzo, A., Ianni, M., Fortino, G., Piccialli, F.: Model aggregation techniques in federated learning: A comprehensive survey. Future Generation Computer Systems 150, 272–293 (2024)

Beltr´an, E.T.M., P´erez, M.Q., S´anchez, P.M.S., Bernal, S.L., Bovet, G., P´erez, M.G., P´erez, G.M., Celdr´an, A.H.: Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. IEEE Communications Surveys & Tutorials (2023)

Yang, M., Guo, T., Zhu, T., Tjuawinata, I., Zhao, J., Lam, K.-Y.: Local differential privacy and its applications: A comprehensive survey. Computer Standards & Interfaces, 103827 (2023)

Shakya, A.K., Pillai, G., Chakrabarty, S.: Reinforcement learning algorithms: A brief survey. Expert Systems with Applications 231, 120495 (2023)

Abel, D., Barreto, A., Van Roy, B., Precup, D., Hasselt, H.P., Singh, S.: A definition of continual reinforcement learning. Advances in Neural Information Processing Systems 36 (2024)

Zakariah, M., AlQahtani, S.A., Alawwad, A.M., Alotaibi, A.A.: Intrusion detection system with customized machine learning techniques for nsl-kdd dataset. Computers, Materials & Continua 77(3) (2023)

Yuliana, Y., Supriyadi, D.H., Fahlevi, M.R., Arisagas, M.R.: Analysis of nslkdd for the implementation of machine learning in network intrusion detection system. Journal of Informatics Information System Software Engineering and Applications (INISTA) 6(2), 80–89 (2024)

Vibhute, A.D., Khan, M., Patil, C.H., Gaikwad, S.V., Mane, A.V., Patel, K.K.: Network anomaly detection and performance evaluation of convolutional neural networks on unsw-nb15 dataset. Procedia Computer Science 235, 2227–2236 (2024)

Kumar, A., Guleria, K., Chauhan, R., Upadhyay, D.: Advancing intrusion detection with machine learning: Insights from the unsw-nb15 dataset. In: 2024 IEEE International Conference on Information Technology, Electronics and Intelligent

Communication Systems (ICITEICS), pp. 1–5 (2024). IEEE

Phulre, A.K., Verma, M., Mathur, J.P.S., Jain, S.: Approach on machine learning techniques for anomaly-based web intrusion detection systems: Using cicids2017 dataset. In: International Conference on MAchine inTelligence for Research & Innovations, pp. 59–72 (2023). Springer

Guo, G., Pan, X., Liu, H., Li, F., Pei, L., Hu, K.: An iot intrusion detection system based on ton iot network dataset. In: 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0333–0338 (2023). IEEE

Abdusalomov, A.B., Nasimov, R., Nasimova, N., Muminov, B., Whangbo, T.K.: Evaluating synthetic medical images using artificial intelligence with the gan algorithm. Sensors 23(7), 3440 (2023)

Garcea, F., Serra, A., Lamberti, F., Morra, L.: Data augmentation for medical imaging: A systematic literature review. Computers in Biology and Medicine 152, 106391 (2023)

Ali, T.E., Chong, Y.-W., Manickam, S.: Machine learning techniques to detect a ddos attack in sdn: A systematic review. Applied Sciences 13(5), 3183 (2023)

Vistro, D.M., Hassan, T., Ullah, Z.: Ransomware malware: Attacks and preventions. In: AIP Conference Proceedings, vol. 2802 (2024). AIP Publishing

Qiu, W., Yin, H., Wu, Y., Zeng, C., Chen, C., Dong, Y., Liu, Y.: Data security defense: Modeling and detection of synchrophasor data spoofing attack for grid edge. In: 2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5 (2024). IEEE

Zapzalka, D., Salem, S., Mohaisen, D.: Semantics-preserving node injection attacks against gnn-based acfg malware classifiers. IEEE Transactions on Dependable and Secure Computing (2024)