International Research Journal of Multidisciplinary Scope (IRJMS), 2025; 6(2): 1480-1494 IRJMS

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2025.v06i02.03768

Deep Learning for Anomaly Detection in IoT Healthcare Systems

Ahmad shah Mirkhail*, Zhang Xinyou

School of Computer and Artificial Intelligence, Southwest Jiaotong University, Chengdu, China. *Corresponding Author's Email: ahmadshahmirkhail@gmail.com

Abstract

This study introduces a new hybrid deep learning method for intrusion detection in the Internet of Medical Things (IoMT), a rapidly expanding domain that enhances patient care but remains highly vulnerable to cyber threats. The increasing integration of IoMT devices in healthcare facilitates real-time monitoring and data exchange, yet their susceptibility to security breaches poses serious risks to patient privacy and system integrity. As these devices generate vast amounts of sensitive data, ensuring security against cyberattacks is critical. Our proposed method integrates an Autoencoder (AE) with three encoder-decoder layers for anomaly detection and a Long Short-Term Memory (LSTM) network for temporal analysis. The autoencoder identifies anomalies through reconstruction errors and latent space classification, while the LSTM network captures sequential patterns in network traffic to detect attack signatures. We evaluated the model using the CICIoMT2024 data set, which includes traffic from 40 IoMT devices and 18 distinct attack types across Wi-Fi, MQTT, and Bluetooth protocols. The data set presents a significant class imbalance, with DoS and DDoS attacks dominating, posing real-world security challenges. To address this, we employed data balancing techniques to improve model performance. Our evaluation shows that the hybrid model achieves 94.1% accuracy with a robust Area Under the Curve (AUC), significantly outperforming the Autoencoder alone. Our findings demonstrate the efficacy of employing deep learning techniques to bolster IoMT security. This approach enables swift identification of various cybersecurity threats and establishes a resilient defense system against emerging attacks.

Keywords: Autoencoder (AE), Deep Learning, Intrusion Detection System (IDS), Internet of Medical Things (IoMT), Internet of Things (IoT), Long Short-Term Memory (LSTM).

Introduction

The swift development of the Internet of Things (IoT) is altering everyday life by interconnecting billions of devices that have sensing, communication, and processing functionalities (1, 2). These interconnected gadgets are being utilized for health monitoring, enabling real-time surveillance of patients' health metrics (3, 4). The Internet of Medical Things (IoMT) emerged from the convergence of the Internet of Things (IoT) with healthcare with the goal of revolutionizing healthcare services by way of individualized treatment programs and real-time tracking (5). A number of acronyms make up the IoMT, which stands for the Internet of Medical Things; these include "MIoT" and "H-IoT" (6, 7). IoMT systems provide conveniences to various users, including patients through wearable technologies, healthcare professionals through quick patient information access, and administrative personnel through the administration of medicinal assets. The Internet of Medical Things (IoMT) encompasses various subcategories, including Body Area Network (BAN), Wireless Body Area Network (WBAN), Body Sensor Network (BSN), and Wireless Medical Sensor Network (WMSN). These systems are collectively recognized as specialized networks within the broader IoMT framework (8). The healthcare sector produces vast amounts of data that conventional approaches find challenging to analyze it. Machine learning (ML) and Deep Learning (DL) methods offer automated techniques that enhance the extraction of essential features for data analysis, particularly from electronic health records (9). Machine learning (ML) and deep learning (DL) techniques provide advanced capabilities for data analysis, predictive analytics, and the personalization of medical treatments (10). Data security and privacy are critical because of the utilization of digital technologies like IoT, mobile gadgets, and medical

(Received 11th January 2025; Accepted 15th April 2025; Published 30th April 2025)

cloud computing, where breaches may result in financial losses and erosion of trust. Encryption, blockchain and biometric systems have been used to enhance the security (11). Healthcare IoT devices face security risks due to vulnerabilities across hardware (physical tampering, side-channel attacks, counterfeit components, insufficient tamper resistance), software (poor coding, inadequate patching, limited security features due to resource constraints), and network layers (eavesdropping, unauthorized access, man-in-the-middle attacks via Wi-Fi, Bluetooth, ZigBee, issues during network transitions, weak key management and routing protocols like RPL, and DoS/DDoS attacks). These vulnerabilities necessitate strong security measures and proactive design approaches for reliable and safe healthcare IoT systems (12). IoMT systems are vulnerable to cyberattacks, which can compromise patient privacy, infrastructure integrity, and operational continuity, including data breaches, denial-of-service and manipulation of medical data (13). Loss of diagnostic information due to security breaches in healthcare systems can have a negative effect on diagnosis, treatment, and even patient lives (14). For the aim of detecting malicious actions, intrusion detection systems (IDS) are important, using methods, such as those based on signatures, anomalies and specifications and hybrid approaches (15). While several methodologies have been presented for detecting intrusion in IoT based healthcare systems, their effectiveness is evolving continuedly. Several research have examined machine learning (ML), deep learning (DL), and combined methods, all with the goal of optimizing the precision and reliability of malicious activity detection. The current research outlines diverse approaches for threat detection in IoT systems. These techniques can be commonly categorized into three major types: machine learning-based approaches, deep learning-based models, and hybrid strategies that integrate both. Machine learning models are one such method to identify the intrusion in IoT healthcare system. It was observed that four supervised machine learning techniques, namely Naive Bayes, Decision Tree, K-Nearest Neighbors (KNN), and Random Forest were applied, to classify attacks in two data sets, namely, CICIDS2017 and Bot-IoT. The precision and F1-scores obtained for Naive Bayes 42%, 41%, Decision Tree 93.2%, 93%, KNN 91%, 91%, Random Forest 93.3%, 94% were reported in the CICIDS2017 data set. For the Bot-IoT data set, the precision and F1-scores were: Naive Bayes (91%, 91%), Decision Tree 99%, 99%, KNN (98.9%, 98%), Random Forest 98.7%, 98% (16). It was found that three supervised machine learning techniques, namely Artificial Neural Network (ANN), Decision Tree, and K-Nearest Neighbors (KNN), were applied to classify attacks in the IoTID20 dataset. The reported precision and F1-score values are as follows: for ANN, 99% precision and 98% F1-score; for Decision Tree, 99% precision and 99.8% F1-score; and for KNN, 99.2% precision and 99% F1-score (17). It was demonstrated that different machine learning methods to enhance the potency of intrusion detection systems. In particular, it has been observed that Decision Tree together with AdaBoost and K-Nearest Neighbour (KNN) and Random Forest models were employed. The performance metrics include that a precision of 99.6% alongside F1 score of 99.8% were achieved by the Decision Tree while, a precision of 99.8% with an F1 score of 99.9% was attained by AdaBoost. The results confirm the capacity of these methods to increase the accuracy and trustworthiness of intrusion detection system in real time (18). However, it has been noted that deep learning models such as RNNs and DNNs are of interest for learning complex structure in the large dataset. Intrusion Detection System based on Deep Neural Network It was proposed that an Intrusion Detection System based on a Deep Neural Network can achieve efficient performance metrics. Using the NF UQ NIDS data set, it was found that the model achieved a precision of 93.02% and an F1 score of 91.76% in multiclass classification tasks, thereby demonstrating its capability for real-time detection of various network assaults. It was further demonstrated that the model is capable of meeting the challenges commonly encountered by typical IDS, which often fail when faced with diverse and dynamic network traffic (19). It was proposed that an efficient method exploiting a Deep Neural Network (DNN) model be used to identify anomalies. The model was designed to enhance the security of IoT networks by accurately classifying network traffic as normal or abnormal. It was found that the DNN model was superior, achieving an F1 score of

98.6% and a precision of 99%. It was further concluded that this approach substantially strengthens the performance of network-based intrusion detection systems in IoT environments by detecting anomalies with a minimal false alarm ratio (20). It was noticed that a CNN-based system was designed to detect environmental sensor anomalies within healthcare IoT ecosystems. The model was tested through the WSN DDoS Attack H-IoT2023 dataset which was developed using the Cooja simulator platform. The CNN model architecture was optimized for one-dimensional time-series inputs and evaluated using accuracy and error rate metrics. A 92% accuracy rate was achieved by the model, with models like SVM, LSTM, and ensemble learning being outperformed in both efficiency and precision (21). An anomaly-based intrusion detection system (AIDS) for the Internet of Medical Things (IoMT) was created by applying six ML and DL algorithms, which included RF, SVC, KNN, CNN, CNN-LSTM, and attention-based CNN-LSTM. In this research, the TON_IoT telemetry dataset was used to study different cyberattacks, including DDoS, ransomware, and scanning activities. SMOTE was applied to the training data in order to handle class imbalance. The evaluation of each model was based on accuracy, precision, recall, and F1-score metrics. The best accuracy results of 99% were achieved by Random Forest together with KNN, while attention-based CNN-LSTM achieved 94%. The CNN-LSTM model was observed to perform poorly (22). As observed healthcare systems intrusion detection method was introduced that combined Correlation-based Feature Selection with Bat Optimization Algorithm (HCFS-BOA) alongside Convolutional Neural Networks (CNN). Both the CIC-IDS2017 and NSL-KDD datasets were used, to which min-max normalization was applied and HCFS-BOA was utilized for feature selection based on correlation and optimization. CNN was employed to perform intrusion classification following the feature selection process (23). It was demonstrated that the Eccentric Intrusion Detection Model (EIDM), which employs Recurrent Neural Networks (RNNs) with Long Short-Term Memory (LSTM) units, is capable of detecting several cyberattack scenarios, including both conventional and unique attacks. The model was trained and tested on the CICIDS2019 data set, which comprises various benign and malicious network traffic examples. It was found that the proposed models achieved detection fidelity of 99.5% and a very low false positive rate of 72%, indicating a strong capability to support cybersecurity systems for intrusion detection (24). It was reported that a novel intrusion detection solution for IoT settings, based on a Denoising Autoencoder (DAE), was proposed. The CICIDS 2017 and NSL-KDD data sets were applied to assess the model. In the CICIDS 2017 data set, the DAE achieved a precision of 99.9% and an F1-score of 98%, while in the NSL-KDD data set, a precision of 94% and an F1-score of 98.9% were obtained. These findings validate that the model is capable of successfully detecting intrusions and can be used to enhance security in IoT systems (25). Recently, multiple intrusion detection models have been hybridized to obtain the strength of the individual models and improve the precision. For instance, AE-LSTM-CNN is presented as a hybrid deep learning framework that is aimed at boosting intrusion detection capabilities in IoT systems. Autoencoders with LSTMs along with CNNs are used by the integrated model to perform multi-stage feature extraction in order to detect multiple attack forms. This hybrid mode was evaluated on the CICIoT2023 dataset and an accuracy and F1-score of 99.1% were achieved (26). It was reported that a hybrid IDS for Internet of Medical Things (IoMT) was developed by integrating Gated Recurrent Units (GRU) with Attention Mechanisms to enhance detection of known and unknown as well as zero-day attacks. When tested on the ICU Healthcare and NF-TON-IoT datasets, accuracy levels of 99.99% and 98.94% were reached by the model, together with precise measurements and high recall scores on both datasets, thereby proving its reliable real-time operation (27). JAYA-BiLSTMIDS on the IoT-23 data set yielded a precision of 99.6%, and a precision of 99.88% was obtained on the MQTT set data set (28). It was introduced that a hybrid deep learning strategy for Internet of Medical Things (IoMT) system intrusion detection is proposed. Three models—including the proposed GNN-BiLSTM, GRU-BiLSTM, and CNN-BiLSTM—are tested using the 'IoT healthcare security' dataset. The GNN-BiLSTM model is shown to exhibit the best performance with 99.98% accuracy and 99.97% F1 score compared to GRU-BiLSTM (99.95% accuracy, 99.94% F1 score) and CNN-BiLSTM (99.97%

accuracy, 99.96% F1 score). Moreover, the GNN-BiLSTM is found to be much more efficient with the classification task. It is demonstrated that the GNN-BiLSTM serves as an effective IoMT security solution because it delivers strong accuracy alongside quick processing times (29). It was employed a two-tier intrusion detection system including a stacked autoencoder (SAE) for feature retrieval and a deep neural network (DNN) for classification. This model was assessed applying three multiclass datasets: KDDCup99, NSL-KDD, and AWID. The multiclass accuracies attained were dependent on the dataset and the count of layers in the DNN; however, the optimal model (a DNN with two layers) attained roughly 94.2% precision on the KDDCup99 dataset, 99.7% on the NSL-KDD dataset, and 99.9% on the AWID dataset. It was noted that the paper did not clearly disclose F1-scores for multiclass categorization (30). This paper proposes a new hybrid deep learning approach for intrusion detection in the context of IoMT that combines an Autoencoder with a Long Short-Term Memory network using weighted ensemble approach. Compared to previous studies that have usually carried out features extraction or time dependent pattern analysis in network traffic, our method integrates these two strategies to identify important features and temporal variations. Furthermore, we also tackle the inherent class imbalance of the CICIoMT2024 dataset to have equal representation of all attack types via oversampling and under sampling techniques. The evaluation metrics show robust performance with accuracy reaching 94.1% and excellent ROC AUC scores. The study results confirm the effectiveness of our methodology by addressing critical gaps within current research on Internet of Medical Things security.

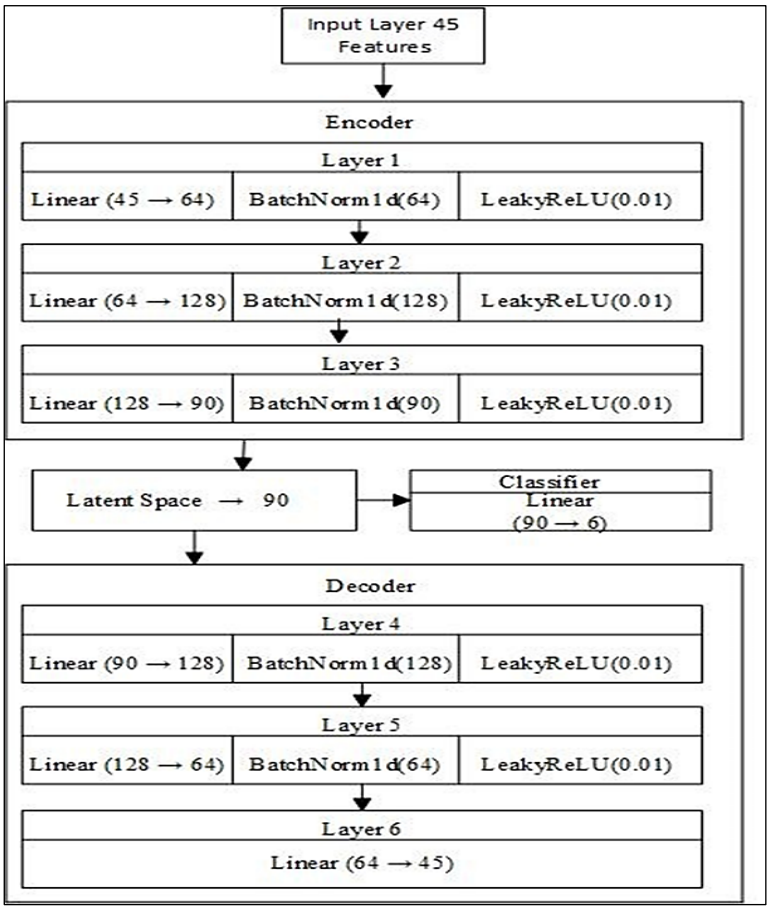

Figure 1: Autoencoder Model with 6 Layers

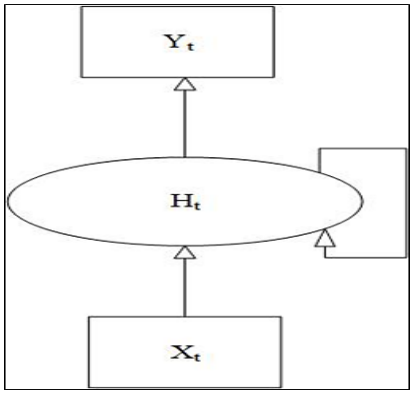

Figure 2: RNN Fold Representation

Methodology

In this section, we elucidate the methodologies of hybrid AutoEncoder and Long Short-Term-Memory LSTM. We demonstrate our suggested model, named hybrid Autoencoder method combined with the LSTM model for security violation detection in IoT based healthcare. In the subsequent section, we will explain how each component of our proposed model work. The hybrid AutoEncoder (AE), (LSTM), and the weighted ensemble of both models. The reconstruction error is applied by the Autoencoder model to determine if IoT network traffic is normal or aberrant (31). Our work introduces autoencoder architecture with a classification head, three layers of encoders, and three layers of decoders. Following batch normalization and the LeakyReLU activation function, each encoder and decoder layer is a dense layer. Classification predictions are generated by the classification head using the latent space, allowing the model to execute reconstruction and classification at the same time. Figure 1 illustrates the Autoencoder (AE), whereas Figure 2 represents the LSTM model.

Autoencoder Method

An autoencoder (AE) is an algorithm that compresses data into a representation with minimal dimensions through an encoder and subsequently recreates this compressed version to approximate the original version input through a decoder component. The autoencoder consists of two components, namely an encoder and a decoder. The encoder transforms the initial data into a finite depiction, termed to as the encoding layer or latent space layer, whilst the decoder reconstructs the initial data from this encoding layer. Encoders and decoders frequently perform linear operations that can be executed unsupervised within a dense layer of a neural network. The encoder converts the input x into a latent representation h, whereas the decoder reconstructs the initial data as $\hat{x}$ from h. An encoder is a deterministic aligning function $f(x)$ that transforms a multidimensional input matrix x into an r-dimensional latent representation h, known as an encode, as illustrated below:

$$h = f(x) = \phi(wx + b) = sigmoid(wx + b) = \frac{1}{1 + e^{-(wx+b)}} \text{ [1]}$$

A decoder is an operation of mapping (h) that transforms the latent form h, derived from Equation [1], into a reconstructed vector z within the input space. A decoder can also be expressed as an affine transformation followed by a squashing linearity, as depicted below:

$$z = g(h) = \phi(w\hat{h} + \hat{b}) = sigmoid\ (w\hat{h} + \widehat{b)} = \frac{1}{1 + e^{-(\hat{w}h+\hat{b})}} \text{ [2]}$$

Where wˆ represents the weight matrix of the affine mapping and bˆ denotes the bias vector, while $\phi(h)$ signifies the activation function referred to as the sigmoid function. Generally, the learning process in autoencoders involves optimizing the weights to minimize the reconstruction error (32). As a result, the objective function can be represented as follows:

$$\varphi = \| x - \hat{x} \| \text{ [3]}$$

For anomaly detection task, autoencoders have the advantage of learning efficient representations of data and are able to detect deviations from normal patterns that may signal potential threat. In healthcare specifically, this capability is important for early detection of anomalies in order to save patient lives.

Recurrent Neural Network

Unlike basic neural networks like Multilayer Perceptions (MLPs), Recurrent Neural Networks (RNNs) are not limited to single-directional input processing. Recurrent Neural Networks (RNNs) can loop multiple layers and possess the ability to temporarily retain information for future use. The architecture of a Recurrent Neural Network (RNN) is illustrated in Figure 2.

H_t Signifies a hidden layer, X_t identifies the input, and Y_t represents the output. RNNs are classified as deep neural networks due to the multiple layers involved in input processing. Figure 3 illustrates the unfolding structure of a standard RNN to demonstrate the depth of the RNN architecture.

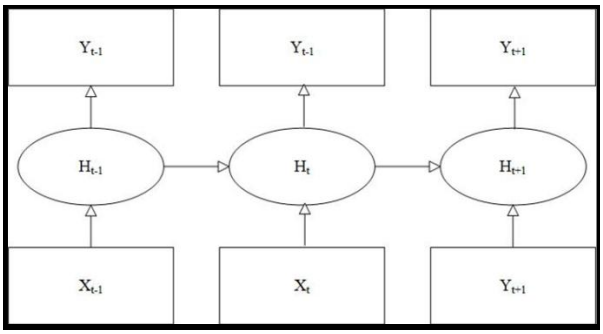

Figure 3: RNN Unfold Representation

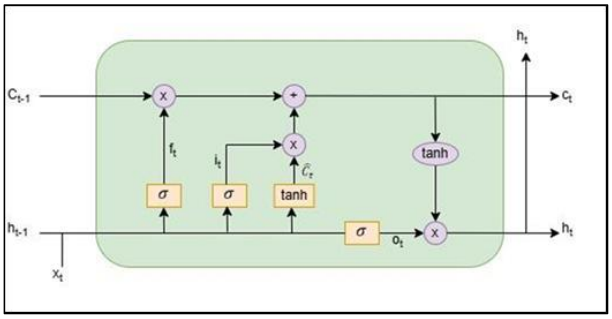

Figure 4: LSTM Memory Cell Structure

X_{t-1} denotes previous input, H_{t-1} denotes previous hidden layer, Y_{t-1} denotes previous output, and X_t represent current input, H_t represent current hidden layer, Y_t represent current output, and X_{t+1} indicates next input, H_{t+1} indicates next hidden layer, Y_{t+1} indicates next output (33).

Long short-term Memory

Long Short-Term Memory (LSTM) networks are a specific type of recurrent neural networks (RNNs) designed to mitigate the limitations of traditional RNNs in handling long-term interdependencies in sequential data. Standard RNNs experience the vanishing and exploding gradient problem, when gradients decrease progressively at the time of backpropagation across time, resulting in network's inability to retain information from previous time steps. This significantly limits their capacity to discern patterns over extended periods, a crucial constraint for tasks like speech recognition or machine translation. Figure 4 shows the LSTM cell architecture which, address this issue by the utilization of an advanced cell architecture and gating mechanism. The core element of LSTM is its memory cell, a system designed to preserve information for prolonged durations. This cell engages with three essential gates: an input gate that regulates the inflow of input data, a forget gate that decides which information from the prior cell state should be eliminated, and an output gate that modulates the extent to which the cell's current state is disclosed as the network's output. The gates, in conjunction with the cell state, facilitate precise regulation of information flow within the network, permitting LSTMs to acquire and maintain information over considerably longer sequences than conventional

RNNs, thereby effectively mitigating the vanishing gradient issue and enhancing their capability for intricate sequential data processing (34). The current input data point x_t and the disguised state from the previous time step h_{t-1} are the two inputs that the LSTM cell receives. Forget Gate f_t This gate supervise which information should be removed from the cell's memory. The prior hidden state h_{t-1} and the current input x_t are utilised as inputs. A sigmoid activation function (σ) compresses the output to a range betwixt 0 and 1, with 0 indicating entirely discard and 1 signifying entirely preserve.

$$f_t = \sigma\left(w_f . (h_{t-1}, x_t) + b_f\right) \quad [4]$$

Input Gate i_t the input gate specifies how much of new data from the current input x_t and prior hidden state (h_{t-1}) that should be stored in the cell state. A sigmoid function (σ) is applied to assess the significance of this fresh information.

$$i_t = \sigma(w_i . (h_{t-1}, x_t) + b_i) \quad [5]$$

Candidate cell state $C_t\hat{}$ this is the new possible content that will be included in the cell state It is calculated as a function of the input at the present time step x_t and the preceding hidden state h_{t-1} passed through a tanh function. The tanh ensures the values remain in the of range (-1,1).

$$\widehat{C_t} = tanh(w_c . (h_{t-1}, x_t), + b_c) \quad [6]$$

Cell state update C_t the cell state is modified by summing the preceding cell state C_{t-1} and the candidate cell state $C_t\hat{}$ the forget gate f_t control the extent to which the prior cell state is preserved while the input gate i_t regulate the amount of the candidate cell state $Ct\hat{}$ to be included. The result is the new cell state C_t

$$C_t = f_t . C_{t-1} + i_t . \widehat{C_t} \quad [7]$$

Output gate O_t the output gate determines which parts of the updated cell state C_t are used to compute the hidden state h_t. The output importance is decided by applying a sigmoid function.

$$o_t = \sigma(w_o . (h_{t-1}, x_t) + b_o) \quad [8]$$

The hidden state h_t is computed by passing the updated cell state C_t through a tanh function to squash the values in the range of (-1,1) and modulated by the output gate o_t. This hidden state is used as output and passed to the next time step.

$$h_t = o_t . tanh(C_t) \quad [9]$$

The Long Short-Term Memory (LSTM) networks are particularly well suited for learning from sequential data, and therefore, are ideal to identify patterns and anomalies over time in the context of healthcare monitoring. This model can effectively process time series data and can detect a slight deviation from normal and abnormal behavior that may indicate a possible intrusion. Such capability not only improves the reliability of the health monitoring systems but also allows timely detection of intrusion, thus improving the patient outcomes and safety in critical care environments. An effective approach for detecting anomalies in IoT-based healthcare systems is represented by the integration of Autoencoder and LSTM models. The Autoencoder's capacity for efficient representation and deviation detection, combined with the LSTM's strength in modeling sequential data and capturing subtle temporal variations, results in a robust detection system. A robust detection system is formed by the combination of the Autoencoder's efficient representation and deviation detection capabilities with the LSTM's strength in modeling sequential data and capturing subtle temporal variations. The unique challenges posed by high-dimensional, time-series healthcare data are effectively addressed by this hybrid approach, ensuring timely and reliable anomaly detection.

Dataset

This study utilizes the CICIoMT2024 data set to evaluate performance of the hybrid AutoEncoder (AE), (LSTM), and the weighted ensemble of both models. in identifying cyberattacks targeting Internet of Medical Things (IoMT) devices. The CICIoMT2024 data set comprises information from 40 IoMT devices, composed of 25 real and 15 imitated devices. This multi-protocol data set contains 18 unique attack types across Wi-Fi, MQTT, and Bluetooth, comprising Denial of Service (TCP, ICMP, SYN, UDP), Distributed Denial of Service (TCP, ICMP, SYN, UDP), reconnaissance (Ping Sweep, OS Scan, Port Scan, Vulnerability Scan), MQTT attacks (Malformed Data, DoS Connect Flood, DoS Publish Flood, DDoS Connect Flood, DDoS Publish Flood), and ARP Spoofing. The data set is notably imbalanced, showing a substantially greater number of instances for DoS and DDoS attacks relative to other attack types and benign traffic (35). As detailed in Table 1, this represents the number of attack instances in each class.

Table 1: Number of Attack Instances in Each Class of Cisiomt2024 Data Set

Class	Category	Attack	Count
Benign	-	-	200339
Attack	Spoofing	ARP Spoofing	17791
		Ping Sweep	926
	Recon	Recon VulScan	3207
		OS Scan	20666
		Port Scan	106603
		Malformed data	6877
		DoS connect flood	15904
		DDoS publish flood	36039
	MQTT	DoS publish flood	52881
		DDoS connect flood	214952
		DoS TCP	462480
		DoS ICMP	514724
	DoS	DoS SYN	540498
		DoS UDP	704503
		DDoS SYN	974359
		DDoS TCP	987063
	DDoS	DDoS ICMP	1887175
		DDoS UDP	1998026

Consequently, we aggregated all specific attack types into their main categories to streamline classification and manage the complexity arising from numerous sub-categories. For instance, specific attack types for DoS and DDoS, like DoS TCP, DoS ICMP, and DoS SYN, were consolidated under the broader classifications of DoS and DDoS. Furthermore, subcategories for reconnaissance attacks, including OS Scan and Port Scan, merged into a singular category named Recon. By integrating them into the superior category level taxonomy, we diminished the problem's complexity, hence facilitating subsequent analyses and modelling endeavors to be significantly more manageable and relevant. This effectively preserves the fundamental characteristics of each primary category while enhancing models' capacity to identify generalized patterns in closely related attack types. Following the aggregation of subcategories into main categories, a Label Encoder was applied to convert categorical class labels into numerical values, facilitating accessibility for our machine learning models. A Standard Scaler was then applied to normalize the feature distributions, ensuring that all characteristics maintained equal importance throughout comparable numerical ranges during training. This enhanced model convergence, stability, and overall performance. The data set is highly imbalance, with classes such as TCP_IP-DDoS and TCP_IP-DoS considerably outnumbering others like Spoofing and Recon, hence jeopardizing model bias. To rectify this, we employed oversampling and under sampling methods to guarantee equitable representation of all classes—TCP_IP-DDoS, TCP_IP-DoS, Benign, Recon, Spoofing, and MQTT. Specifically, random under sampling techniques were applied to decrease the over-represented classes including TCP_IP-DDoS and TCP_IP-DoS whereas random oversampling techniques were used to increase under-represented classes like Spoofing and Recon. This procedure implemented a fixed random seed to achieve perfect data division where the training and testing sets included 1,066,764 samples for each class. This method supplied sufficient data for the model to identify the distinctive characteristics of minority classes while preventing the predominance of majority classes. The model's generalization, fairness, and robustness enhanced, resulting in improved assessment metrics and more dependable performance in identifying various risk within the network. and testing set. This method supplied sufficient data for the model to identify the distinctive characteristics of minority classes while preventing the predominance of majority classes. The model's generalization, fairness, and robustness enhanced,

resulting in improved assessment metrics and more dependable performance in identifying various risk within the network.

Experiment setting

A Windows 10 (64-bit) machine with an Intel Core i9-12900K CPU, 32 GB of RAM, and an NVIDIA RTX 4060 graphic processing unit (GPU) with 8 GB of dedicated memory was used for the research. The PyCharm integrated development environment (IDE) made use of the PyTorch framework for building and running the proposed model. In order to carry out and evaluate the experimental procedures described in this work efficiently, this configuration offered the necessary processing power and adaptability.

Results

The model was trained for a total of 50 epochs to avert overfitting, before each training epoch begins, the data are shuffled to prevent the model from learning any sequence patterns that aren't intended. Partitioning the data into smaller batches of a predetermined size (e.g., 64 samples each batch) is the next step. By randomly sorting and batching data at each epoch, we may optimize the model's generalizability and accelerate the training process In Figure 5, the left diagram displays the accuracy of hybrid autoencoder, while the right graph shows the loss of hybrid autoencoder, whereas in Figure 6, the left graph represents the accuracy of LSTM model, and the right graph presents the loss of LSTM model. The training results demonstrate that the LSTM Classifier surpasses the Hybrid Autoencoder model. Despite an increase in the Hybrid Autoencoder's training precision, its testing precision remained low and inconsistent, indicating a decrease in training loss alongside a high and fluctuating testing loss. This indicates poor generalization to novel data. The LSTM Classifier showed constant improvements in both training and testing precision, in addition to decreases in training and testing loss, highlighting its outstanding generalization and overall performance on the task model.

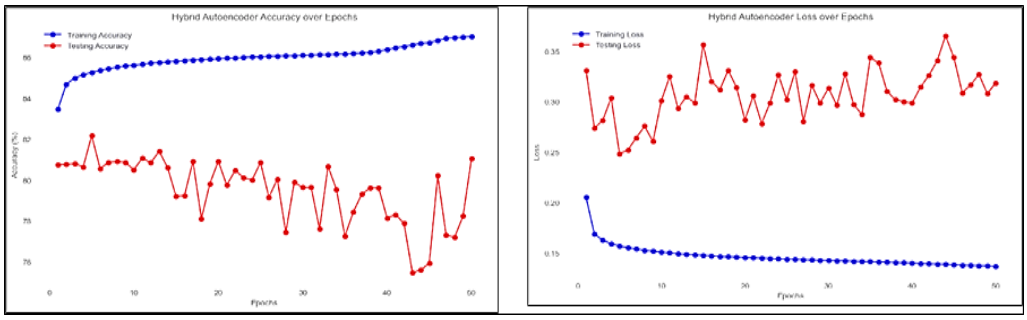

Figure 5: Hybrid Autoencoder Accuracy over Epochs-Hybrid Autoencoder Loss over Epochs

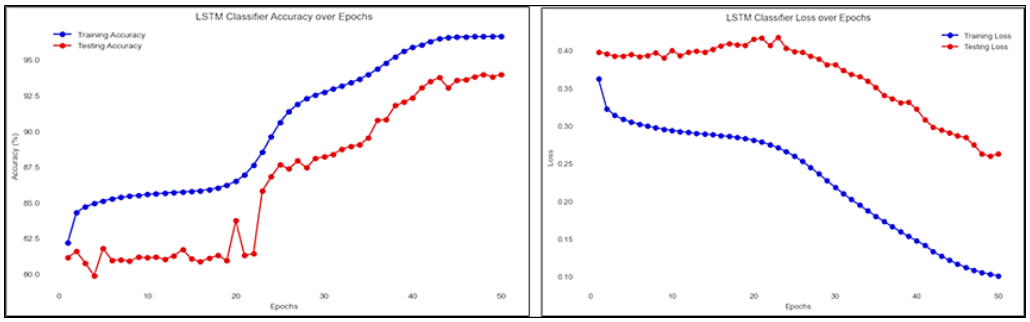

Figure 6: LSTM Classifier Accuracy over Epochs-LSTM Loss over Epochs

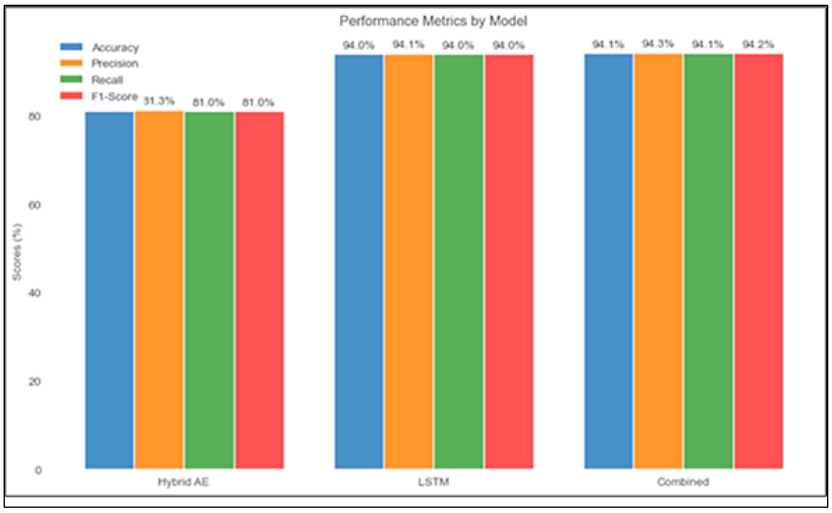

Figure 7: Performance Metrics by Model

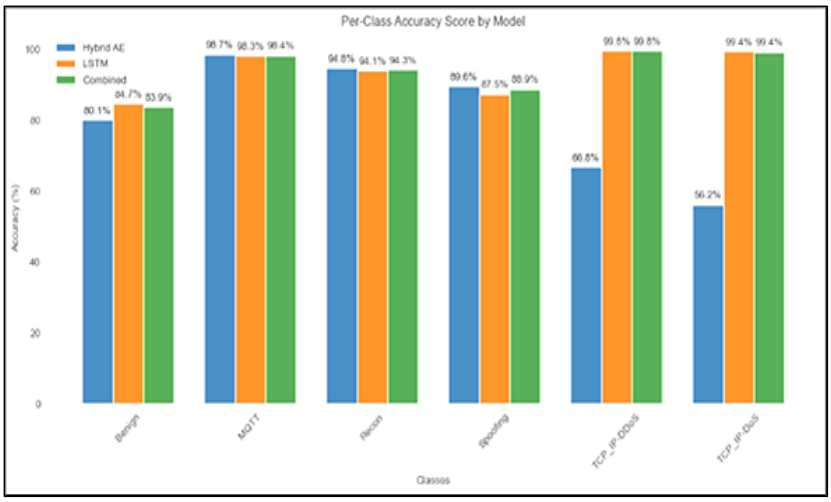

Figure 8: Per Class Accuracy by Model

In Figure 7, we display per-class accuracy by model, and in Figure 8, we represent the per-class accuracy by model as we evaluate the performance metrics of three models: Hybrid AE, LSTM, and Combined for intrusion detection in IoT-based healthcare. The performance measures demonstrate that the LSTM and Combined models much outperform the Hybrid AE model in precision, precision, recall, and F1-score, with both the LSTM and Combined models attaining roughly 94% for each metric, in contrast to the Hybrid AE's 81%. The LSTM and Combined models show similar overall performance; however, the combined model indicates marginally superior precision at 94.1% compared to the LSTM model's 94.0%, along with a marginally higher recall of 94.1% compared to 94.0%. The marginal increase in performance is evident in the second chart, where the Combined model attains slightly superior precision in the "Benign," "Recon," and "Spoofing" classes. This stands in stark contrast to the Hybrid AE's performance, which remains at approximately 81% across all parameters, indicating its limited ability to effectively identify intrusion. The overall pattern is accentuated by the analysis of per-class precision, wherein the LSTM and Combined models consistently exhibit superior performance across all traffic classes, particularly in the "TCP_IP-DDoS" and "TCP_IP-DoS" classes. The Hybrid AE model exhibits a notable decline in precision for those classes, whereas the LSTM and Combined models attain above 99% precision, indicating that the Hybrid AE is less effective in classifying these traffic categories in comparison to the other models. Nevertheless, although the combined model demonstrates marginally excellent. The Table 2 ROC curve performance metrics encapsulates the successful implementation of the combined model across various classes taking advantage of ROC

curves. The AUC (Area Under the Curve) assesses capability of the model to differentiate between true positives and false positives for each class, with a greater AUC signifying superior performance. The Table 2 ROC curve performance metrics illustrates that the model exhibits outstanding performance, with AUC values. Between 98% and 100%. The model attains impeccable AUC scores of 1.00% for classes such as MQTT, Recon, TCP_IP-DDoS, and TCP_IP-DoS, indicating flawless discrimination without any errors. The Benign and Spoofing classes exhibit AUC values of 98%, indicating exceptional performance with little misclassifications. The Table 2 ROC curve performance metrics highlights the model's robust classification capability across multiple classes, exhibiting excellent precision and reliability.

Table 2: ROC Curve Performance Metrics

Class	AUC (Area Under Curve)	Performance
Benign	98%	excellent
MQTT	100%	Perfect
Recon	100%	Perfect
Spoofing	98%	excellent
TCP_IP-DDoS	100%	Perfect
TCP_IP-DoS	100%	Perfect

Table 3: Performance Comparison with Other Methods

Method	Precision	Recall	F1-score	Accuracy
Weight average (36)	85%	84%	84%	483%
DNN (37)	74.7%	81.7%	75.3%	81.7%
LSTM (38)	92%	94%	79%	79%
CFS (39)	89%	87%	86.4%	90.3%
BiLSTM (40)	91.1%	89.7%	89.4%	91.9%
AE-LSTM (41)	90.9%	89.7%	89.4%	92%
Our proposed model Weighted Ensemble	94.3%	94.1%	94.2%	94.1%

Table 4: Model Performance Comparison across 5-Fold Cross-Validation

Fold	Hybrid AE Accuracy	LSTM Accuracy	Combined Accuracy
1	85.58%	86.13%	86.10%
2	85.55%	96.40%	96.36%
3	85.46%	95.96%	95.12%
4	85.56%	86.17%	86.07%
5	85.54%	86.19%	86.16%
Mean	85.54%	90.17%	89.96%
Std	0.04%	4.91%	4.73%

Our model's performance was compared to that of other similar models. Using Accuracy, precision, recall, and F1 score for comparison It was observed that the weighted ensemble model achieved the highest F1-score of 94.1% and an accuracy of over 94.1%, as shown in Table 3. We conducted a 5-fold cross-validation to compare the performance of three models: Hybrid Autoencoder (Hybrid AE), LSTM, and a Combined (ensemble) approach. Table 4 summarizes the accuracy results.

Throughout all folds the Hybrid AE system demonstrated reliable performance with accuracy rates at 85.5% which indicates its overall reliability and robustness. The LSTM and Combined methods demonstrated peak accuracy levels at 96.40% and 96.36% in folds 2 and 3 but displayed more unstable performance measures throughout the entire process. To determine whether the performance differences among the

three models were statistically significant, we performed a non-parametric Friedman test. This test compares the models' ranks across the folds rather than their exact accuracy values. The Friedman test yielded a chi-square statistic of 10.00 and a p-value of 0.0067. Since this p-value is less than 0.05, we conclude that there are statistically significant differences in the models' performances. The LSTM and Combined models display performance metrics that are statistically different from the Hybrid AE model which demonstrates consistent moderate results. The experimental results indicate that LSTM models detect specific data patterns well although they deliver peak accuracy inconsistently between different data subsets while the Hybrid AE model maintains steady and reliable performance.

Discussion

This research employs Autoencoder (AE) and Long Short-Term Memory (LSTM) networks because of their complementing advantages. LSTM networks are especially applicable for processing sequential data and capturing long-term dependencies, which is critical for detecting patterns in time-series data like network traffic. The forget gate in LSTM is essential for deciding which data to preserve or eliminate, allowing the model focusing on important information and identify changing attack patterns such as DDoS and DoS, which are extremely dynamic and necessitate long-term pattern recognition. Autoencoders (AE), on the other hand, are excellent in feature extraction because they learn compressed representations of input data. Autoencoder detects anomalies through reconstruction errors thus proving highly efficient for discovering security breaches by tracking abnormal traffic patterns. The Autoencoder algorithm shows better results at finding defects in data but performs worse when used for time-based inputs compared to LSTM. The hybrid AE-LSTM model band together the attributes of AE models with LSTM models to extract features and detect anomalies and analyze sequential patterns therefore achieving better identification of sophisticated network attack patterns. The preprocessing procedures started with handling missing data then followed standard scaling of features and attack type consolidation to simplify the classification process. The analysis integrates DoS TCP, DoS ICMP and DoS SYN attacks under the headers of DoS and Distributed Denial of Service (DDoS). The OS Scan and Port Scan reconnaissance attacks have been placed into the "Recon" classification group. Combining attack types into broader groups made the data set easier to process while keeping essential aspects of each assault type to help the model recognize typical patterns. The application of Label Encoder processed categorical class labels for numerical transformation in order to make them compatible with machine learning models. In addition, oversampling and under sampling techniques were used to address the class imbalance so that all the attacks get fair representation and the model becomes fair, robust, and have better generalization capability. Our weighted ensemble of Autoencoders and LSTM networks produced strong results when identifying different cyber-attacks especially Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS) and reconnaissance activities. This approach lets the models work separately and combine their results for decision-making. The AE model learns compact representations of relevant features of the data and the LSTM model extracts temporal information from one sequential traffic. After the predictions of both models have been generated, these predictions are integrated using the weighted ensemble method which weights the contribution of each model based on its performance. By using this method, the hybrid model can take advantage of the strength of both techniques, where the Autoencoder has the ability to extract features and the LSTM has the capacity to seize long term dependency within the data. Attacks are categorized effectively by this method into diverse specific types such as 'TCP-IP-DDoS' and 'TCP-IP-DoS' and by 'Recon' and 'Spoofing' while distinguishing normal from malicious traffic. The weighted ensemble method delivers accurate results that make it advisable for real-time detection of network threats in IoMT systems. The results in Table 3 compare the Weighted Ensemble model against six state-of-the-art methods (Models 33-38) The results show that the Weighted Ensemble greatly performs better than any other model with precision of 94.3%, recall of 94.1%, F1-score of 94.2%, and accuracy of 94.1%. The experimental results show our method enhances the detection ability while improving upon the performance strength of separate

baseline models when used for IoT-based anomaly detection. The ensemble's superiority stems from its capability to bring together different architectures which effectively mitigating weaknesses present in single models. The extensive analysis shows how the proposed approach can lead the development of new methods in healthcare anomaly detection systems. As shown in Table 4, the results are a tradeoff between stability and peak performance. It was found that the Hybrid Autoencoder (Hybrid AE) model was consistently reliable and had an accuracy of 85.5 percent. This shows that it will be a good choice for applications where stability is the prime concern. Although the combined and LSTM models were better able to reach higher peak accuracies at 96.4% and 96.36, respectively, it was the single model that achieved the highest overall accuracies at 95.5%. However, these models were more variable across folds which indicates that they are more sensitive to the data used. The results from the Friedman test at $p = 0.0067$ proved the performance differences between models were statistically significant where the LSTM and Combined models showed superior performance compared to Hybrid AE. The performance of LSTM and Combined models results in better accuracy levels when compared to Hybrid AE. The primary focus of research is on anomaly detection in IoMT system, but we acknowledge that an adversarial attack where an attacker aims to manipulate input data to mislead the model can also expose the model in reducing detection accuracy and increase false negatives. Our method combining an Autoencoder with an LSTM has the potential to resist small adversarial perturbations because it detects anomaly from typical patterns that were learned during training. The present study did not implement dedicated defenses against adversarial attacks. Future research of IoMT anomaly detection systems needs specific hazard resistance techniques such as adversarial training because this remains an essential research topic to enhance the healthcare security. Future research should aim to further enhance the resilience and adaptability of IoMT anomaly detection systems. One promising direction is the integration of dedicated adversarial defense mechanisms, such as adversarial training or robust optimization techniques, to mitigate potential attacks designed to bypass the current detection framework. Additionally, expanding the dataset to include a wider variety of IoMT devices and attack types could improve model generalization and enable the development of more sophisticated, real-time detection systems. Finally, exploring alternative or hybrid deep learning architectures, as well as the fusion of additional data modalities (e.g., contextual patient data), may provide further insights and lead to more robust and comprehensive security solutions for IoMT environments.

Conclusion

In order to study the effectiveness of an Autoencoder (AE), Long Short-Term Memory (LSTM) network, and their combination, a novel innovative breach detection system for Internet of Medical Things (IoMT) environments was introduced and evaluated in this research. Numerous key results were obtained from experimental findings on the CICIOMT2024 data set. Autoencoder model had potential but the best findings were based on the LSTM model. In the case of all these parameters of accuracy, precision, recall, and F1-score the LSTM model showed its robustness with exactly 94%. The most conspicuous and remarkable outcomes were achieved using the combined method, which combined the merits of the AE and LSTM. By combining these two approaches, we achieved over 99% precision on most of the traffic categories including the most important ones, TCP_IP-DDoS and TCP_IP-DoS, and outperformed the performance of each individual model. This indicates that the combined method can protect medical IoT devices effectively. Moreover, Receiver Operating Characteristic (ROC) Curve research demonstrated that the combined model had extremely high efficacy across multiple classes with Area Under the Curve values of 100%. Further validation of our approach was carried out with 5-fold cross validation, and a non-parametric Friedman test was applied to show that the difference of the models' performance was statistically significant with a chi square statistic of 10.00 ($p = 0.0067$). The results show that a combination of the AE and LSTM models is a sturdy and efficient way for intrusion detection. The use of this combined strategy offers a solid foundation for enhancing reliable security systems designed to resolve the particular challenges that emerge in

the IoT-based healthcare environment. Further study of this model will be placed toward its real time application and further refinement for usage in multiple medical settings.

Abbreviations

AE: AutoEncoder, AUC: Area Under the Curve, CNN: Convolutional Neural Network, DDoS: Distributed Denial of Service, DoS: Denial of Service, IoMT: Internet of Medical Things, LSTM: Long Short-Term Memory, RNN: Recurrent Neural Network, ROC: Receiver Operating Characteristic.

Acknowledgement

The author acknowledges the dedication, perseverance, and self-motivation that made this research possible.

Author Contributions

All authors contributed equally.

Conflict of Interest

There is no conflict of interest.

Ethics Approval

Not applicable.

Funding

This research was funded by Southwest Jiaotong University to cover the publication costs.

References

1. Li C, Wang J, Wang S, Zhang Y. A review of IoT applications in healthcare. Neurocomputing. 2024; 565:127017.
2. Shehada D, Gawanmeh A, Yeun CY, Zemerly MJ. Fog-based distributed trust and reputation management system for internet of things. J King Saud Univ-Comput Inf Sci. 2022;34(10):8637-46.
3. Muthukrishnan A, Kamalesh S. IOT device type identification using magnetized Hopfield neural network with tuna swarm optimization algorithm. Swarm Evol Comput. 2024;91:101653.
4. Kronlid C, Brantnell A, Elf M, Borg J, Palm K. Sociotechnical analysis of factors influencing IoT adoption in healthcare: a systematic review. Technol Soc. 2024:102675.
5. Wakili A, Bakkali S. Internet of Things in healthcare: An adaptive ethical framework for IoT in digital health. Clin eHealth. 2024;7:92-105.
6. Dimitrov DV. Medical internet of things and big data in healthcare. Healthc Inform Res. 2016;22(3):156-63.
7. Kumar M, Kumar A, Verma S, Bhattacharya P, Ghimire D, Kim S-h, et al. Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues. Electronics. 2023;12(9):2050.
8. Nezhad MZ, Bojnordi AJJ, Mehraeen M, Bagheri R, Rezazadeh J. Securing the future of IoT-healthcare systems: A meta-synthesis of mandatory security requirements. Int J Med Inform. 2024;185:105379.
9. Swain S, Bhushan B, Dhiman G, Viriyasitavat W. Appositeness of optimized and reliable machine learning for healthcare: a survey. Arch Comput Methods Eng. 2022;29(6):3981-4003.
10. Badawy M, Ramadan N, Hefny HA. Healthcare predictive analytics using machine learning and deep learning techniques: a survey. J Electr Syst Inf Technol. 2023;10(1):40.
11. Singh AK, Anand A, Lv Z, Ko H, Mohan A. A survey on healthcare data: a security perspective. ACM Trans Multimed Comput Commun Appl. 2021;17(2s):1-26.
12. Tsantikidou K, Sklavos N, editors. Vulnerabilities of Internet of Things, for Healthcare Devices and Applications. 2021 8th NAFOSTED Conference on Information and Computer Science (NICS); 2021: IEEE.
doi: 10.1109/NICS54270.2021.9701497
13. Kondeti V, Bahsi H, editors. Mapping Cyber Attacks on the Internet of Medical Things: A Taxonomic Review. 2024 19th Annual System of Systems Engineering Conference (SoSE); 2024: IEEE.
doi:10.1109/SOSE62659.2024.10620925
14. Srivastava K, Faist K, Lickert B, Neville K, McCarthy N, Fehling-Kaschek M, et al. editors. Assessment of the Impact of Cyber-Attacks and Security Breaches in Diagnostic Systems on the Healthcare Sector. 2024 IEEE International Conference on Cyber Security and Resilience (CSR); 2024: IEEE.
doi: 10.1109/CSR61664.2024.10679475
15. Heidari A, Jabraeil Jamali MA. Internet of Things intrusion detection systems: a comprehensive review and future directions. Cluster Computing. 2023;26(6):3753-80.
16. Mittal S, Mishra AK, Tripathi V, Singh P, Pandey P, editors. A comparative analysis of supervised machine learning models for smart intrusion detection in IoT network. 2023 3rd Asian Conference on Innovation in Technology (ASIANCON); 2023: IEEE.
doi: 10.1109/ASIANCON58793.2023.10270377
17. Albulayhi K, Abu Al-Haija Q, Alsuhibany SA, Jillepalli AA, Ashrafuzzaman M, Sheldon FT. IoT intrusion detection using machine learning with a novel high performing feature selection method. Applied Sciences. 2022;12(10):5015.
18. Hidayat I, Ali MZ, Arshad A. Machine learning-based intrusion detection system: an experimental comparison. Journal of Computational and Cognitive Engineering. 2023;2(2):88-97.
19. Vishwakarma M, Kesswani N. DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT. Decision Analytics Journal. 2022;5:100142.
20. Ahmad Z, Shahid Khan A, Nisar K, Haider I, Hassan R, Haque MR, et al. Anomaly detection using deep neural network for IoT architecture. Applied Sciences. 2021;11(15):7050.
21. Khatun MA, Bhattacharya M, Eising C, Dhirani LL, editors. Time Series Anomaly Detection with CNN for Environmental Sensors in Healthcare-IoT. 2024 IEEE 12th International Conference on Healthcare Informatics (ICHI); 2024: IEEE.
https://doi.org/10.48550/arXiv.2407.20695
22. Franklin E, Pranggono B. Anomaly-Based Intrusion Detection System for the Internet of Medical Things.

IJID (International Journal on Informatics for Development).12(2):374-85.
23. Bella HK, Vasundra S. Healthcare Intrusion Detection using Hybrid Correlation-based Feature Selection-Bat Optimization Algorithm with Convolutional Neural Network: A Hybrid Correlation-based Feature Selection for Intrusion Detection Systems. International Journal of Advanced Computer Science & Applications. 2024;15(1). doi:10.14569/ijacsa.2024.0150166
24. Muthunambu NK, Prabakaran S, PrabhuKavin B, Siruvangur KS, Chinnadurai K, Ali J. A Novel Eccentric Intrusion Detection Model Based on Recurrent Neural Networks with Leveraging LSTM. Computers, Materials & Continua. 2024;78(3): 3089-3127. https://doi.org/10.32604/cmc.2023.043172
25. Alrayes FS, Zakariah M, Amin SU, Khan ZI, Helal M. Intrusion detection in IoT systems using denoising autoencoder. IEEE Access. 2024;99:1-1.
26. Susilo B, Muis A, Sari RF. Intelligent Intrusion Detection System Against Various Attacks Based on a Hybrid Deep Learning Algorithm. Sensors. 2025;25(2):580.
27. Saran N, Kesswani N. Intrusion detection system for internet of medical things using gru with attention mechanism-based hybrid deep learning technique. Jordanian Journal of Computers and Information Technology (JJCIT). pp. 136 – 150. doi: 10.5455/jjcit.71-1725609265.
28. Dash N, Chakravarty S, Rath AK. Deep learning model for elevating internet of things intrusion detection. Int J Electr Comput Eng. 2024;14(5):5874-83.
29. Rbah Y, Mahfoudi M, Fattah M, Balboul Y, Mazer S, Elbekkali M, et al. editors. Deep Learning for Enhanced IoMT Security: A GNN-BiLSTM Intrusion Detection System. 2024 International Conference on Circuit, Systems and Communication (ICCSC); 2024: IEEE. DOI:10.1109/ICCSC62074.2024.10616456
30. Muhammad G, Hossain MS, Garg S. Stacked autoencoder-based intrusion detection system to combat financial fraudulent. IEEE Internet of Things Journal. 2020;10(3):2071-8.
31. Xu W, Jang-Jaccard J, Singh A, Wei Y, Sabrina F. Improving performance of autoencoder-based network anomaly detection on nsl-kdd dataset. IEEE Access. 2021;9:140136-46.
32. Nasser M, Salim N, Saeed F, Basurra S, Rabiu I, Hamza H, et al. Feature reduction for molecular similarity searching based on autoencoder deep learning. Biomolecules. 2022;12(4):508.
33. Kasongo SM. A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. Computer Communications. 2023;199:113-25.
34. Shewalkar A. Performance evaluation of deep neural networks applied to speech recognition: RNN, LSTM and GRU. Journal of Artificial Intelligence and Soft Computing Research. 2019;9:235-245.
35. Dadkhah S, Neto ECP, Ferreira R, Molokwu RC, Sadeghi S, Ghorbani A. Ciciomt2024: Attack vectors in healthcare devices-a multi-protocol dataset for assessing iomt device security. Raphael and Chukwuka Molokwu, Reginald and Sadeghi, Somayeh and Ghorbani, Ali, CiCIoMT2024: Attack Vectors in Healthcare Devices-A Multi-Protocol Dataset for Assessing IoMT Device Security. 2024. DOI:10.2139/ssrn.4725150
36. Awotunde JB, Abiodun KM, Adeniyi EA, Folorunso SO, Jimoh RG, editors. A deep learning-based intrusion detection technique for a secured IoMT system. International Conference on Informatics and Intelligent Applications; 2021:50-62. Springer. DOI:10.1007/978-3-030-95630-1_4
37. Hussain J, Hnamte V, editors. A novel deep learning based intrusion detection system: Software defined network. 2021 International Conference on innovation and intelligence for informatics, computing, and technologies (3ICT); 2021: IEEE. doi:10.1109/3ICT53449.2021.9581404
38. Mushtaq E, Zameer A, Umer M, Abbasi AA. A two-stage intrusion detection system with auto-encoder and LSTMs. Applied Soft Computing. 2022;121:108768.
39. Udas PB, Karim ME, Roy KS. SPIDER: A shallow PCA based network intrusion detection system with enhanced recurrent neural networks. Journal of King Saud University-Computer and Information Sciences. 2022;34(10):10246-72.
40. Imrana Y, Xiang Y, Ali L, Abdul-Rauf Z. A bidirectional LSTM deep learning approach for intrusion detection. Expert Syst Appl. 2021;185:115524.
41. Van HT, Nguyen PTMH, editors. Intrusion Detection based on extracting Optimization Features for Bidirectional Long-Short-Term-Memory. Proceedings of the 2024 9th International Conference on Intelligent Information Technology; 2024. https://doi.org/10.1145/3654522.365456