A NOVEL INTRUSION DETECTION MODEL FOR CRITICAL HEALTHCARE ENVIRONMENTS

Aishvarya shree.V.G [1], M.Thangaraj [2] and M. Nirmala Devi [3]

[1] Research scholar, Department of Computer Science, Madurai Kamaraj University Madurai, India
[2] Professor and Head, Department of Computer Science, Madurai Kamaraj University Madurai, India
[3] Assistant Professor (Selection Grade), Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai – 625015, India

ABSTRACT

In this study, a deep learning-based model was proposed by combining a sparse autoencoder and a combination of autoencoders with LSTM for feature selection and intrusion detection. Subsequently, the likelihood of attacks was evaluated using an ensemble method. The proposed model employed several functions and addressed current research gaps, such as reducing false positive rates, mitigating model overfitting, addressing data imbalance, and identifying new attack scenarios. The proposed model was tested on benchmark datasets, viz., WUSTL-EHMS 2020, IoT Healthcare Security 2021, and CIC IoMT 2024. The proposed model achieved a perfect detection rate in binary classification of WUSTL-EHMS 2020 and IoT Healthcare Security 2021. The model achieved an accuracy rate of 99.80% (binary) and 90.67% (multiclass) in the CIC IoMT 2024 dataset. In addition, the Matthews Correlation Coefficient (MCC), Cohen's Kappa, and Adversarial Robustness Score (ARS) provided a comprehensive assessment of the model, demonstrating its robustness and applicability in healthcare.

KEYWORDS

Cyber-attacks, Deep learning, Autoencoder, Ensemble model, Weighted Knowledge Graph

1. INTRODUCTION

The Internet of Things (IoT) has undergone rapid development, thereby advancing various industries, including manufacturing, transportation, healthcare, and agriculture. IoT is a network of physical objects that are embedded with sensors, actuators, communication modules, and storage, etc., for connecting and transferring data over the network. IoMT devices save costs, facilitate improved decision-making, remote patient monitoring, and exhibit high performance efficiency; however, the challenges associated with their security must be addressed. IoMT devices face various security threats due to insufficient credential configuration, a lack of encryption, and obsolete firmware. These vulnerabilities expose crucial data to man-in-the-middle attacks, DDoS, and spoofing, among other threats [1], [2].

The integration of IoT in healthcare systems can revolutionize patient care and promote remote patient monitoring. IoMT facilitates remote patient monitoring, which decreases the need for clinicians to intervene directly. And the acquired data can be used for research purposes [3].

Fundamental components of personalized healthcare systems and e-health systems, such as mobile health (mHealth), telehealth, health informatics, and telemedicine. This paper examines

the advanced alternatives in e-health systems, IoT in healthcare, its role, and difficulties [4]. According to Cynerio's "State of Healthcare IoT Device Security 2022" report, over 50% of Internet of Medical Things (IoMT) devices have been exposed to several critical risks, as approximately half of the systems are outdated. The 2023 report similarly concluded that managing, prioritizing, and comprehending such risks should take precedence over achieving zero risk in such IoMT devices [5]. Additionally, the maintenance of medical equipment is challenging due to the vast range of equipment that is vulnerable to cyberattacks; regular calibration is therefore essential. Downtime of these critical devices disrupts workflow. The devices require specific expertise and trained personnel to operate, as well as frequent maintenance.

Security threats associated with IoMT devices and sensors can have significant consequences, including life-threatening situations for patients and negatively impacting healthcare providers by damaging the organization's reputation [6], [7] because such systems have access to critical medical records of patients. These vulnerabilities can be mitigated using measures such as encryption and BitLocker security; however, intrusion detection systems (IDSs), event and log management, and network segmentation are also required to prevent data breaches and enhance data security. An IDS identifies potential cyber threats in real time and has therefore been widely used in IoMT. Next, the advantages and challenges of IoMT are stated below [8], [9], [10], [11]. The benefits of utilizing IoMT are outlined below.

Enhanced patient monitoring and care: With IoMT, patients' vital signs and movements are tracked in real-time, significantly reducing their need for hospital visits. This technology is widely used to monitor and provide timely updates on chronic health conditions, such as diabetes and cardiovascular diseases, enabling prompt medical responses.

Data-driven decision-making: The information gathered by IoMT devices can be leveraged for healthcare analytics without any data loss, which minimizes manual errors and accelerates the accuracy of decision-making.

Cost reduction: By enabling remote monitoring, IoMT reduces the frequency of hospital visits, enhances operational efficiency, and enables healthcare organizations to manage their resources more effectively.

Encourages research: IoMT devices collect vast amounts of sensitive data that can be utilized to advance medical research and foster innovation.
IoMT devices have these challenges

Real-time data: Enormous processing power is required to generate a wealth of real-time data continuously. Additionally, the history of this data cannot be disregarded, as health-related information is essential for making informed decisions.

Lack of industry and technology exposure: Many end-users are unaware of the latest technological advancements and the security measures that accompany them.

Data security and privacy: Since IoMT devices collect real-time data, it is essential to ensure their security; however, most devices do not adhere to established protocols and standards, which heightens the risk of cyber threats.

Multiple connected devices: The integration of numerous IoMT devices without data loss remains a significant challenge.

Lack of licensed software and resource constraints: A significant amount of software, including electronic health record systems and security applications, is unlicensed and has limited resources, leading to data theft and mismanagement. These challenges can be mitigated by utilizing open-source software and cloud services.

Overall, IoMT has transformed the healthcare industry by exchanging real-time data among medical equipment. Real-world incidents, such as Medjack [12] and vulnerabilities in pacemakers [13], highlight real-time attack scenarios. Most baseline approaches are often tested on traditional network datasets [14]; however, these models lack complexity and fail to handle the diversity of recent IoMT threats. However, this proposed approach is validated using comprehensive benchmark datasets, such as WUSTL-EHMS2020, IoT Healthcare Security 2021, and CIC-IoMT2024, which include realistic spoofing attacks, ensuring that the proposed approach is compatible and robust against current and emerging threats. Moreover, the existing IDS has a high misclassification rate with a significant false positive rate; this is an important issue to consider when incorporating IDS with critical infrastructure, such as the healthcare domain. To overcome these issues, a prototype is proposed that achieves high performance with low loss and misclassification. The structure of this paper is organized as follows: Section 2 reviews pertinent literature and identifies existing research gaps. Section 3 outlines the proposed framework and methodology, while Section 4 presents the extensive experimental results and performance assessment, providing a thorough insight into the framework's capabilities. Finally, Section 5 wraps up the study.

2. LITERATURE REVIEW

Akshay Kumaar et al. [15] proposed a hybrid architecture, ImmuneNet, to identify recent intrusion attacks and secure healthcare data. ImmuneNet uses feature engineering techniques and oversampling to improve class balance. It employs hyperparameter optimization to achieve high accuracy and performance on the Canadian Institute for Cybersecurity (CIC) IDS 2017 and 2018 datasets, as well as the Bell DNS 2021 datasets, ensuring generalizability and robustness. The model achieved an accuracy of ~99.19% for the CIC Bell DNS 2021 dataset. Roy et al. [16] developed a novel IoT intrusion detection model based on B-Stacking, which achieved accuracies of 98.5% and 99.11% on the NSL-KDD and CIC IDS 2017 datasets, respectively. B-Stacking exhibited a high detection rate and low false alarm rate; however, it has to be tested further in real-world IoT scenarios. Alferaidi et al. [17] developed a deep learning-based intrusion detection method for the Internet of Vehicles, achieving 99.7% accuracy in reducing security threats using CNN and LSTM networks.

Raghuvanshi et al. [18] evaluated a model developed for ensuring the security and privacy of agricultural IoT networks using the NSL-KDD dataset. It achieved accuracies of 98%, 85%, and 78% using SVM, RF, and logistic regression, respectively, thereby enabling its real-time implementation in IoT-enabled smart irrigation. Iwendi et al. [19] tested the NSL-KDD dataset using an integrated weighted genetic algorithm with random forest (RF), logistic regression, and naïve Bayes. The genetic model and RF yielded a high detection rate of 98.81% and a low false alarm rate of 0.8%.

Bakro et al. [20] proposed a cloud IDS model that combined an ensemble model with the crow search algorithm (CSA), which exhibited high classification accuracy by selecting better features. This model employed ablation research, which included an ensemble model with and without CSA, and was tested on three datasets: NSL-KDD, Kyoto, and CIC IDS 2018. Without CSA, the accuracy rates were 97.01%, 96.19%, and 98.18%, whereas with CSA, they were 99.01%, 98.99%, and 99.99%, respectively.

Öztürk et al. [21] proposed a model that examined the types of attacks and the performance of supervisory control and data acquisition (SCADA) protocols, which are frequently used in hospitals. This model demonstrated high accuracy when tested on a hardware-in-the-loop water distribution testbed dataset using classification techniques such as K-Nearest Neighbor, Support Vector Machine (SVM), and decision tree techniques. Verma & Ranga [22] proposed a machine learning (ML) classification algorithm to secure IoT systems against denial-of-service (DoS) attacks using popular datasets such as CIDDS-001, UNSWNB15, and NSL-KDD. The algorithm's performance was evaluated using various ensemble methods such as RF, classification and regression trees, multilayer perceptron learning, AdaBoost, gradient-boosted machines, extreme gradient boosting, and extremely randomized trees.

John et al. [23] proposed a security threat detection system that used a cluster-based wireless sensor network and variable-selection ensemble ML algorithm (CBWSN_VSEMLA). It used fuzzy C-means clustering and principal component analysis for feature selection and ensemble ML algorithms for grayhole, blackhole, flooding, and scheduling attacks. The system's performance was evaluated using the WSN-DS dataset. The principal component analysis with random forest outperformed, achieving 99.99% accuracy; however, its computational complexity needs to be reduced. Shambharkar & Sharma [24] proposed three models to address network security issues, namely LinSVM, ConvSVM, and CatEmb, which were tested on the WUSTL-EHMS 2020 dataset. Models achieved training accuracies of 99.78%, 99.98%, and 99.84%, respectively. Zubair et al. [25] proposed a decentralized model for detecting and blocking traffic in the Bluetack dataset, which achieved an F1 score of 97%–99.5% and an accuracy of 99% using a deep neural network (DNN). Goswami et al. [26] proposed the Lion-Salp-Swarm-Optimization Algorithm (LSSOA), which utilizes freely accessible IoT data and combines four optimization techniques: lion, whale, spider monkey, and salp swarm optimization. The LSSOA outperformed other compared approaches with a 99.59% accuracy.

Mosaiyebzadeh et al. [27] proposed a model to detect intrusion in the Internet of Health Things (IoHT) traffic using a DNN and federated learning. The model was tested on the WUSTL-EHMS 2020 and ECU-IoHT datasets, yielding accuracies of 91.40% and 98.47% in anomaly detection; however, the model needs to be evaluated on larger datasets. Hady et al. [28] presented a real-time enhanced healthcare monitoring system testbed that incorporated network and biometric features. The WUSTL-EHMS 2020 dataset was created and evaluated using several ML methods. The SVM model achieved a maximum accuracy of 92.44% and an area under curve (AUC) score of 82.37%, and the artificial neural network (ANN) achieved the highest AUC score of 93.42%. Dadkhah et al. [29] proposed a real-time testbed to enhance the security of IoMT devices. The test bed covered several systems and protocols, and the dataset contained five key attack categories. The dataset was examined using various techniques such as logistic regression, AdaBoost, DNNs, and RFs. RFs and DNNs achieved accuracies ranging from 77% to 99%. Hussain et al. [30] proposed a content-aware IoT security solution for the healthcare domain, which utilized IoT flocking to generate normal and malicious traffic data. The generated dataset was then analyzed using various ML approaches, wherein the RF achieved the highest accuracy of 99.51%. Similarly, this [31] model combines a novel UNet++ and LSTM to categorize attacks in the CIC IoMT 2024 dataset, achieving 87.96% accuracy in attack classification. Benmalek et al [32] introduced a novel AI-driven IDS model that is a stacked model integrated with Multilayer Perceptron (MLP), CNN, and LSTM, examined in WUSTL-EHMS 2020 and IoT Healthcare Security datasets. The model achieved accuracies ranging above 99% in all models.

Shaikh et al. [33] proposed the RCLNet model for intrusion detection, which selects features using RF and recognizes patterns using CNN and LSTM. It employed a self-adaptive attention layer to address specific issues related to IoMT security. The model's performance was evaluated on the WUSTL-EHMS 2020 dataset, yielding an accuracy of 99.78%. Reinforcement learning

can be utilized in the model to enhance intrusion detection rates. Alsolami et al. [34] proposed a model to safeguard healthcare data by employing ensemble learning techniques such as stacking, bagging, and boosting with RF and SVM. The model was tested on the WUSTL-EHMS 2020 dataset, achieving accuracies of 98.88%, 97.83%, and 88.68% using stacking, boosting, and bagging, respectively. Ghourabi [35] proposed a model for intrusion detection in the healthcare IT system using an improved LightGBM and transformer-based model. The model performance was assessed on four different datasets, in which the ECU-IoHT had attack classes relevant to IoHT. The LightGBM and a Bert-based transformed model were tested on four different datasets, yielding an ROC AUC score of over 99%.

Hofer et al. [36] examined the current state and challenges involved in implementing the incremental knowledge graph and proposed the primary graph model to address the identified issues. This model was then used to develop the knowledge graph pipeline and obtain a high-quality knowledge graph, while also providing tools and tactics for knowledge graph building. Chen et al. [37] proposed a knowledge graph as a semantic representation of entities and their attributes. It leveraged joint adaptive embedding to evaluate the quality of the knowledge graph, providing a better representation of word embeddings. Two general datasets and one cybersecurity-related dataset were used for evaluating the knowledge graph. Results revealed an accuracy of 95.8%–91.3%. Li et al. [38] evaluated the quality of a knowledge graph using Neo4j to enhance the existing ontology and create a manually built dataset named CS13K. The quality of the knowledge graph was then assessed using an AttTucker model, which achieved high-dimensional embedding by reducing dimensionality. However, the model must use cyber traffic data to improve the effectiveness of the knowledge graph.

Sarhan & Spruit [39] proposed the Open-CyKG model, which utilizes an attention-based neural open information extraction model to extract relevant information from unstructured reports. This model also used a named entity recognizer to detect triples and word embeddings for fusion, thereby capturing meaningful information and outperforming the existing research works. Future extensions of the model include a multilingual knowledge graph. Gilliard et al. [40] proposed a reasoning model for knowledge graphs in cybersecurity, which comprised three major steps: data preparation, semantic basis, and knowledge graph inference approaches. The proposed model could be applied to applications such as IDS, as it could automatically detect threats and enhance network security. The proposed model is robust, as it can update dynamically. Hao et al. [41] developed knowledge graphs for remote sensing applications. The Protégé tool was used to create the knowledge graph at the mode level based on the extracted data from the text corpus related to remote sensing, and the SPARQL protocol was utilized to describe querying and reasoning in the remote sensing domain. Harnoune et al. [42] utilized biomedical clinical-related data to extract relevant structured information, enabling quick and easy information retrieval about the field, with an 88% accuracy in named entity recognition. Table 1 lists the most popular datasets along with their attack categories. These datasets were generated in synthetic, semisynthetic, and real-world test bed environments.

Table 1. Dataset with classes

Dataset	Classes
DARPA (1998) [43]	DoS, Probe, R2L, U2R, Data
NSL-KDD (2009) [44]	DoS, R2L, U2R, Probe
UNSW-NB15 (2015) [45]	DoS, Analysis, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode, Worms, Backdoor
CICIDS 2017 & 2018 [46]	Brute Force, Heartbleed, Botnet, DDoS, DoS, Web, Infiltration,Port Scan
WSN-DS Dataset (2016) [47]	Flooding, Blackhole, Grayhole, Scheduling Attack

Dataset	Classes
BoT-IoT (2019) [48]	DDoS, DoS, Data theft, Keylogging
TON_IoT (2020) [49]	Scanning, Ransomware, DoS, Injection, Man-in-the-Middle, Malware, Cross site scripting, Backdoor, Password tracking attack
WUSTL EHMS (2020) [28]	Spoofing and Data alteration
CIC -Bell-DNS (2021) [50]	Malware, Phishing, Spam
IoT Healthcare Security(2021) [30]	MQTT DDoS, MQTT publish flood, Brute force, and SlowITE
CIC IoMT dataset (2024) [29]	DDos(SYN, TCP, ICMP,UDP) Dos(SYN, TCP, ICMP,UDP), Recon , ARP Spoofing, MQTT

2.1. Research Gap and Future Directions

Despite significant advancements in IDS technologies, several critical research gaps remain. Traditional methods suffer from high false positive rates and lack the contextual awareness that signature-based detection provides, as it can only look for existing threats. Systems protected this way tend to be susceptible to new ones, including zero-day attacks. To detect sophisticated emerging threats, it is necessary to use contextual awareness. Furthermore, numerous IoMT intrusion detection models have been proposed that rely on general IDS datasets, which overlook the protocol-specific features of IoMT. Deep learning approaches have improved detection accuracy and feature extraction; however, they often face issues such as overfitting, high computational costs, and difficulties in generalizing to heterogeneous, real-world environments. Hybrid models and ensemble methods have further pushed the envelope, but still struggle with scalability and the efficient integration of diverse data sources. Similarly, although knowledge graph-based approaches offer rich semantic representations, challenges in KG completion, data sparsity, and real-time integration limit their practical deployment.

This work addresses these gaps by integrating semantic knowledge graphs with deep learning architectures—specifically, an autoencoder-LSTM framework enhanced with sparse autoencoder-based feature weighting and an Extreme Gradient Boosting ensemble for analyzing attack likelihood. By combining these techniques, our proposed IDS aims to enhance detection accuracy and minimize false positives, while providing robust contextual insights. In addition, our model is evaluated using a benchmark dataset specifically designed for IoMT, providing more realistic insights for healthcare deployments. Future research should focus on refining feature selection strategies, integrating heterogeneous datasets more seamlessly, developing enhanced evaluation metrics, and ensuring real-time adaptability to keep pace with the evolving threat landscapes.

The primary contribution of the proposed model is

- To guarantee scalability, the model is tested on three different datasets.
- The knowledge graph comprises feature groups along with their corresponding weights.
- Anomaly detection utilizes both autoencoder and LSTM, resulting in a very low reconstruction error.
- The model incorporates various techniques, such as Synthetic Minority Oversampling Technique (SMOTE) and early stopping.
- By combining traditional and advanced metrics, our model provides a multidimensional evaluation.
- To assess the likelihood of an attack, an ensemble method known as Extreme Gradient Boosting (XG Boosting) is utilized.

3. PROPOSED FRAMEWORK AND METHODOLOGY

Figure 1 shows the intrusion detection model developed for IoMT devices. The three key layers in its architecture namely the data, semantic, and detection layers have a unique set of functionalities.

The prototype leveraged a real-time dataset generated on a test bed comprising real and simulated devices. This dataset contained data on network traffic generated from IoMT devices. Moreover, the model performance was tested by creating attack scenarios such as distributed DoS (DDoS), DoS, Recon, message queuing telemetry transport (MQTT), and spoofing using real and simulated devices. The features of the network traffic were preprocessed to enhance model performance, and the features were then grouped by various domains.These features were then depicted as knowledge graphs, and the feature weights were determined using a sparse autoencoder. The last layer employed various feature engineering and fine-tuning techniques, as well as deep learning with an ensemble model, for a more precise prediction of intrusions. This prototype focuses on minimizing reconstruction error and loss, and reducing overfitting by employing early stopping to enhance accurate predictions.

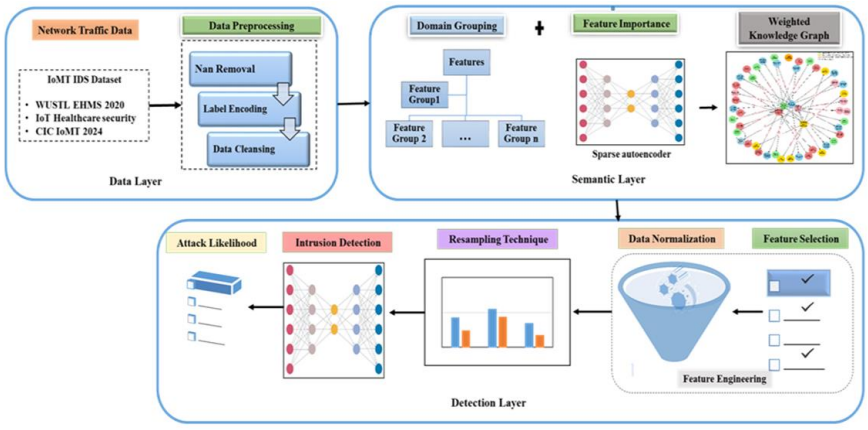

Figure 1. Proposed IDS in IoMT

3.1. Data Layer

In this layer, data analytics approaches were employed to obtain accurate predictions of the real-time benchmark for evaluating model performance. It includes NaN removal, label encoding, and data cleansing, including noise removal using outlier analysis and checks to ensure consistency, thereby ensuring the data is of high quality. The model was evaluated using the most current and up-to-date data obtained from the WUSTL-EHMS 2020, IoT Healthcare Security 2021, and CIC IoMT 2024 datasets, which are ideal for assessing medical device security solutions.

Data preprocessing

Data preprocessing involved two key functions: removing not a number (NaN) values and performing label encoding. Then, data cleansing was performed to obtain clean and noise-free data.

NaN removal involves removing null data and is a vital process when dealing with large datasets. This process considerably improves data quality, increases model performance, and reduces computational load. By removing null data, sparse datasets can be handled, and the risk of model

overfitting can be reduced. The proposed model uses the dropna () function in pandas to remove unwanted data. Next, Label encoding converts categorical features into numerical features, assigning each attack type a distinct numerical value for intrusion detection. Label encoding can be easily implemented and is highly efficient when handling large amounts of data compared to one-hot encoding, as it reduces the data size.

Data cleansing removes noisy data by deleting extraneous information, eliminating random errors, and removing repeated header columns. This usually occurs in network traffic logs, which should be removed to improve the generalizability and standard integrity of the dataset. It ensures data quality via a consistency check by examining data types. This process reduces errors during model training and enhances the model's performance. The proposed model was tested on three datasets containing benign data and attacks to ensure that the data were clean, thereby ensuring better model prediction and task performance.

3.2. Semantic Layer

The semantic layer comprises two main components: domain grouping and feature importance. These steps promote a deeper understanding of the features and allow for the analysis of their weights, which is crucial to the intrusion detection process.

Domain grouping

In domain grouping, the features from datasets were categorized based on their attributes, and a feature knowledge graph was constructed—the proposed model used three distinct datasets. Figure 2 illustrates the categories of basic network traffic information, including their key features.

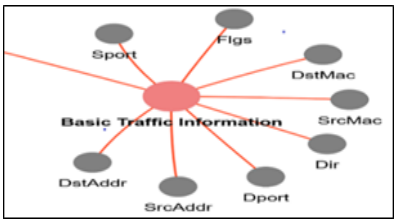

Figure 2. Sample Feature Group

Sparse Autoencoder

A sparse autoencoder consists of multiple dense layers, including an input layer, a hidden layer (encoding phase), a bottleneck layer, a hidden layer (decoding phase), and an output layer, as explained below:

Input layer - It transforms the data into a high-dimensional space by accepting the input feature and applying the activation function (ReLU) with L1 regularization, which adds sparsity to focus on important features.

Hidden layer (encoding phase) - This layer converts the input into a compact, meaningful representation by reducing noise and distortion. It also employs dropout to prevent overfitting and promote generalization. It retrieves fundamental latent features using dimension reduction progression (64 → 32 → 16 → 8).

Bottleneck layer - It represents the compressed form of input with meaningful features.
Hidden layer (decoding phase) - As the progression increases, this layer expands and decodes features to their original dimensions (8 → 16 → 32 → 64).

Output layer - It reflects the reconstructed form of the input, ensuring an accurate representation of the original data.

Feature importance

The weight of each feature was simultaneously computed using a sparse autoencoder, which is an ANN used for learning effective data representation. This ANN introduced a sparsity constraint, allowing the model to utilize only a limited number of neurons at a time. The feature weights were computed by developing a sequential sparse autoencoder model with many layers that used rectified linear unit (ReLU) activation and L1 regularization. The model was then trained by recreating its input layer, during which the weights of each feature were determined using the following techniques.

Weighted knowledge graph

The feature knowledge graph was then merged with the estimated feature weights to create a weighted knowledge graph (Figure 3). In this graph, each feature is linked to its related feature group, with the corresponding weights applied. The graph was developed in an interactive format using the pyvis package, which can be accessed via the following link: weighted knowledge graph contained feature sets and their corresponding weights from three datasets. For instance, the WUSTL-EHMS 2020 dataset contained two significant feature groups: flow metrics and biometric characteristics. Flow metrics were further divided into seven categories, ranging from basic traffic data to loss and error measurements. The IoT healthcare security 2021 dataset comprised five key feature groups: TCP, MQTT, IP characteristics, frame properties, and miscellaneous. The CIC IoMT 2024 dataset comprised four major feature groups: header and packet characteristics, and Open Systems Interconnection layer protocols, categorized as application, transport, and link layers.

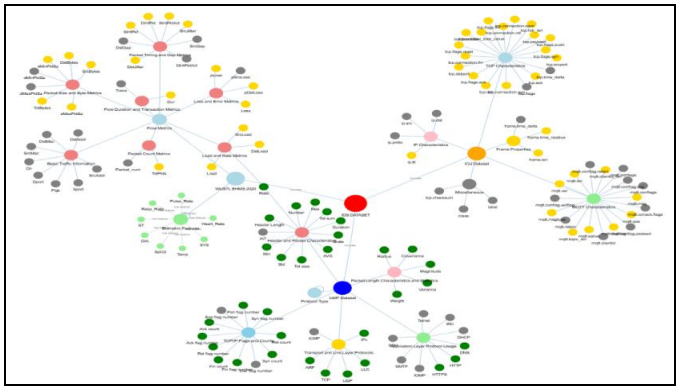

Figure 3. Weighted Knowledge Graph

3.3. Detection Layer

The detection layer employed crucial processes, including feature engineering, resampling techniques, intrusion detection, and attack likelihood analysis, to address class imbalance and classify intrusions with high accuracy.

Feature engineering

Feature engineering is a crucial component of the proposed model, where data transformation and feature selection enable the model to perform more effectively and produce more accurate predictions. During feature selection, the most relevant features in the datasets were selected for processing based on their corresponding weights, calculated by a sparse autoencoder. These features, along with their weights, are represented in the weighted knowledge graph in Figure 3. Data normalization minimizes model inaccuracies and enhances data analytics by scaling the data to a given range using the MinMax equation (Eq. 1). As the IDS dataset contained several features and noisy data, the data were preprocessed during feature engineering before normalization to improve model performance. Labels and class features were excluded during scaling because their normalization caused confusion in the model, leading to misclassification.

$$X_{normalized} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \qquad (1)$$

Resampling technique

Synthetic sampling adjusts the minority and majority classes based on the model's requirements. The data were oversampled using the synthetic minority oversampling technique (SMOTE) with a random_ state of 42. Random Under Sampler was also used to remove superfluous data from the majority class using a random_ state of 42. Additional representative and balanced data were generated, and SMOTE and Random Under Sampler were used to mitigate model overfitting and class imbalance; this process enhanced model generalizability. Sampling techniques were used to prevent semantic data imbalance. In the binary classification process, the before and after sampling categories include two types: attack and benign. However, for multiclass classification, the sampling data covers multiple categories, such as different types of attacks and the benign category, allowing for a broader classification beyond just two classes. Figure 4 shows the process of handling data imbalance using SMOTE across three datasets.

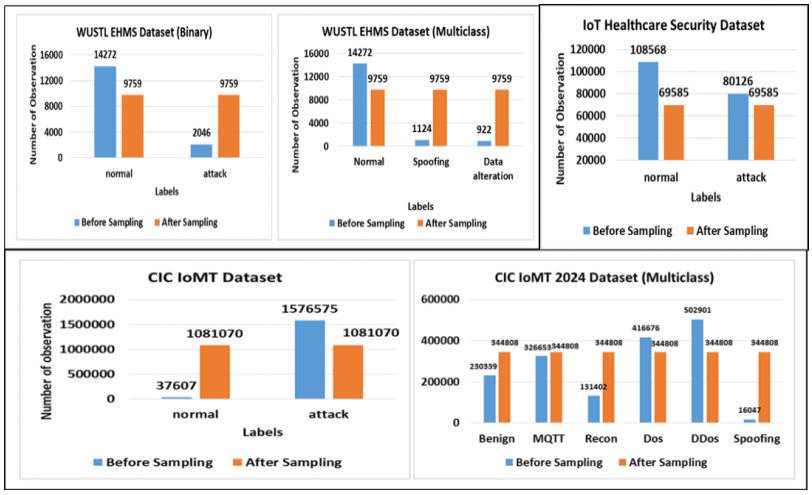

Figure 4. Resampling technique across three datasets

Intrusion detection

Figure 5 illustrates the pipeline employed to detect intrusions in network traffic using a deep autoencoder with LSTM. The three key components in the deep autoencoder enabled the model to learn from compressed input forms. The normalized features were transmitted to the input layer and encoded using three hidden layers with ReLU activation function and three neurons to reduce the dimensionality and extract important features. LSTM integration, a crucial component of the pipeline, comprised an encoder layer with a tanh function, a reshape layer, and an LSTM layer with a ReLU function. The data were reconstructed back to their original form (decoding) using three hidden layers with the ReLU activation function and the output layer with the sigmoid function. The model was then compiled using the Adam optimizer, which manages noisy problems and sparse gradients, along with the loss function. The features of the autoencoder were refined using the LSTM and used in the classification model. These features were defined using the Softmax layer that predicted the class probabilities. Early stopping was introduced in the classification model to reduce overfitting, and a learning rate was used to adjust the learning when the validation loss plateaued. The impact of activation functions, such as ReLU, Tanh, Sigmoid, and Softmax, on enhancing the performance of the proposed model is discussed below.
ReLU: This function is used in the hidden layers of the model, addressing the vanishing gradient problem and promoting effective training. The sparse representation of ReLU facilitates better feature extraction, enabling the model to distinguish easily between malicious and benign data.

$$f(x)=max(0,x) \tag{2}$$

Tanh: The Tanh function helps the autoencoder learn from a balanced representation for intrusion detection, thereby facilitating anomaly detection.

$$\tanh(x) = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}} \tag{3}$$

Sigmoid*:* This function is used in the output layer of the autoencoder. By observing small changes, this function helps the model to identify the features of an intrusion.

$$f(x) = \frac{1}{1 + e^{-x}} \tag{4}$$

Softmax: This function is added to the output layer of multi-classification tasks attached to the autoencoder for classifying intrusions and identifying anomalies. Thus, the proposed model can accurately classify data based on normalized probability across classes.

$$f(x_i) = \frac{e^{x_i}}{\sum_{j=1}^{n} e^{x_j}} \tag{5}$$

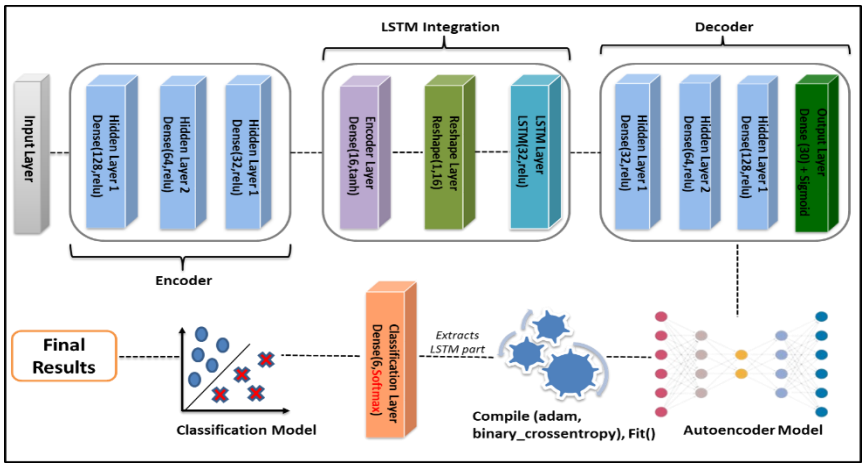

Figure 5. Structure of Autoencoder

Attack likelihood

The extreme gradient boost (XGBoost) ensemble model, developed through 5-fold cross-validation, was used to analyze the likelihood of attacks during multiclass classification. This model was then trained, and predict_proba() determined the likelihood of an attack, returning the probabilities for each class. The result was initially a floating - point number [0, 1], which was then converted into a percentage value and filtered using a threshold value of 0.9 to identify high-likelihood attacks. The numeric labels were then replaced with individual attack names to facilitate better understanding, as well as encourage actionability and reporting.

The WUSTL-EHMS 2020 dataset comprises two attack categories: spoofing attacks (198 observations, indicating a high likelihood) and data alteration (185 occurrences, with a likelihood). The CIC IoMT dataset features five primary attack categories, including DoS, which exhibits a high likelihood range with 100,840 occurrences.

4. EXPERIMENTAL SETUP

The hyperparameters shown in Table 2 were tuned based on the complexity and requirements of the datasets.

Datasets

The model's performance in terms of IoMT security was analyzed by testing it on three real-time benchmark datasets: WUSTL-EHMS 2020, IoT Healthcare Security 2021, and CIC IoMT 2024. These datasets facilitate advanced research on the security of the IoT device in the healthcare sector. They contain various features, and the vital features are chosen based on the previously computed weights during training and testing. The knowledge graph shows features, groups, and their weights.

Table 2. Hyperparameters and its values

Hyperparameter	**Values**	
	Autoencoder	**Classification Model**
Input Dimensions	Number of input features	Same as autoencoder (input_dim)
Hidden Layer Sizes	128, 64, 32, 16 (encoding layer)	128, 64, 32, 32 (LSTM layer)
Activation Functions	ReLU (hidden layers) , Tanh	ReLU (hidden layers), Sigmoid

	(encoding layer)	(output layer)
Regularization	L1 regularizer (10e-5) on encoding layer	-
Optimizer	Adam (learning rate = 0.001)	
Loss Function	Binary Crossentropy	Binary or sparse_categorical_ crossentropy
Batch Size and Epochs	128 and 20	128
Early Stopping	-	Patience of 3, restore best weights
Minimum Learning Rate	-	0.00001
Attack likelihood		
Estimator and scoring	XGBoost Algorithm and Accuracy	
Cross–Fold & Threshold	5 & 0.9	

WUSTL-EHMS 2020 dataset

This dataset [28] was generated in the enhanced healthcare monitoring system test bed, which contains sensor boards that capture patient data. It includes two attack categories: spoofing and data alteration, and 44 features (35 related to network flow, eight related to biometric characteristics)

IoT Healthcare security 2021 dataset

This dataset [30] was generated using IoT flock and contains benign and attack categories. This dataset contains 52 features and four categories of attacks: MQTT-distributed DoS, MQTT publish flood, brute force, and SlowITE attack.

CIC IoMT 2024 dataset

This realistic benchmark dataset [29] was created to evaluate the security of IoMT solutions. Herein, 18 attacks were launched against 40 IoMT devices, which were classified into five categories: DDoS, DoS, Recon, MQTT, and The spoofing. Dataset directory was divided into two subdirectories: Bluetooth (containing the original benign and attack Bluetooth traffic) and profiling (containing data from the power experiment). WiFi_and_MQTT contained actual benign and attack traffic from WiFi- and MQTT-enabled devices, as well as the features extracted during evaluation using ML methods.

4.1. Performance Metrics

Figure 6 illustrates the reconstruction error rates for binary and multiclass tasks, using three datasets. Reconstruction error is the difference between the original input and the reconstructed output. This error is a key statistic in the autoencoder, indicating the model's performance in input reconstruction. During intrusion detection, this error allows the model to distinguish between attack and normal data. For instance, a higher reconstruction error in an autoencoder model indicates that the model is unable to distinguish between attacks and benign data. A low reconstruction error indicates that the autoencoder can efficiently distinguish between attacks and benign data. The CIC IoMT dataset exhibited a higher reconstruction error rate of 0.2342 for multiclass classification, indicating that the autoencoder model struggled to handle a large number of classes, and 0.2586 for binary classification.

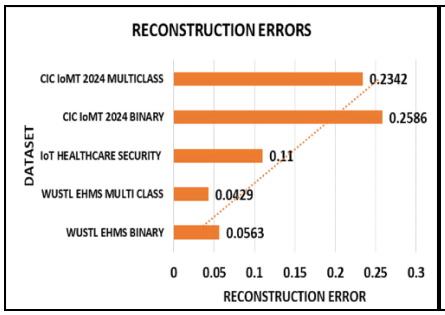

Figure 6. Reconstruction error

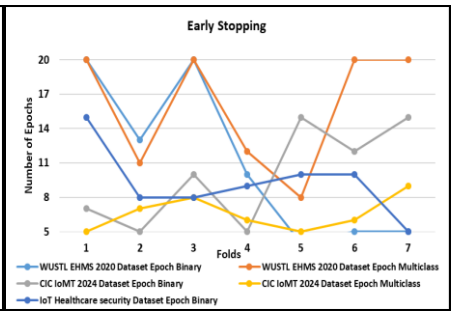

Figure 7. Early Stopping

Figure 7 illustrates the number of epochs per fold in various datasets. The EarlyStopping callback monitors the validation loss and terminates model training when the loss stops decreasing. If the model performance does not improve during future epochs, training will be terminated because the patience value is set to three. By setting restore_best_weights to true, the model's optimal weights were restored. The maximum value for an epoch was 20, and the number of folds was 7 in the proposed model. Early stopping enhances model performance and saves training time by reducing model overfitting and the number of epochs required.

The loss function minimized the difference between the true labels and the predicted probabilities. The proposed model utilized binary cross-entropy and sparse categorical cross-entropy as the loss functions for binary and multiclass classifications, respectively. These loss functions work well with imbalanced data, which is a common anomaly detection strategy. When regularizers were combined with cross-entropy, overfitting was reduced and better model generalization was obtained.

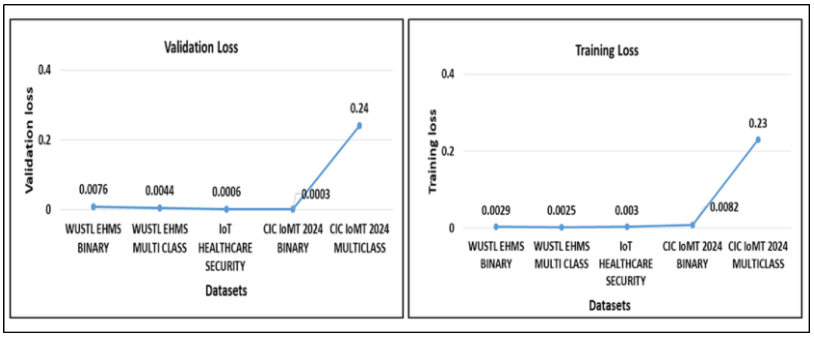

Figure 8. Loss Values

Figure 8 shows the average training and validation loss values for each dataset in binary and multiclass classifications. The minimal loss scores indicated that the model exhibited a low loss level during training and validation. The proposed model fits the data well, providing precise predictions. When experimenting with multiclass classification on the CIC IoMT dataset, the model produced a loss value of 0.23–0.24. This indicated that the loss value was appropriate for the multiclass classification problem. Despite providing accurate predictions, the model failed to classify some classes in the dataset.

The confusion matrix was used to visualize the performance of the proposed model. The binary classification consisted of two classes: benign data and attack, whereas multiclass the classification involved different types of attacks and benign data. Figure 9 shows the confusion

matrix, wherein the binary and multiclass classification results for the WUSTL-EHMS 2020 dataset are shown (Class 0: Benign, Class 1: Spoofing, and Class 2: Data alteration).

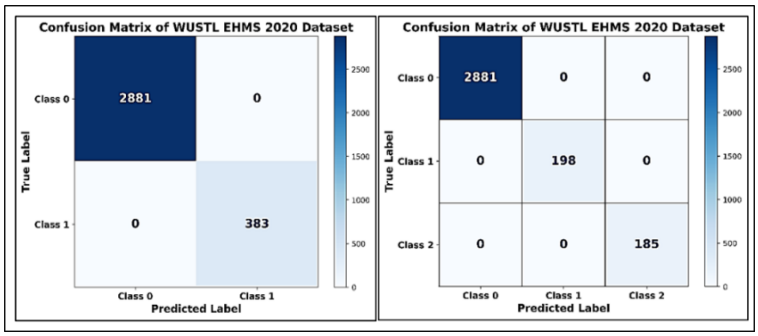

Figure 9. WUSTL EHMS 2020 - Confusion matrix

On the IoT healthcare security 2021 dataset, the proposed approach classified the intrusions more accurately. Figure 10 shows the confusion matrix for evaluating the binary classification

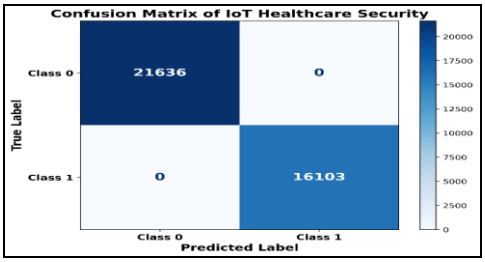

Figure 10. IoT Healthcare Security – Confusion matrix

Figure 11 illustrates the confusion matrix for the CIC IoMT 2024 dataset, demonstrating both binary and multiclass classification. Multiclass classification comprised five different types of attacks and benign data, specifically Class 1: MQTT, Class 2: Recon, Class 3: DoS, Class 4: DDoS, and Class 5: Spoofing.

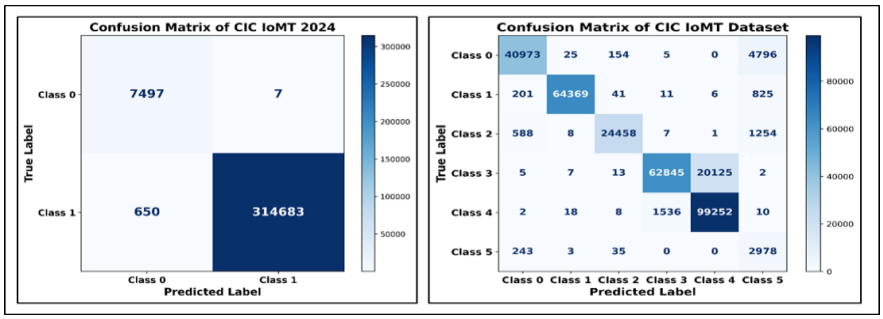

Figure 11. CIC IoMT Dataset - Confusion Matrix

Classification report of the binary and multiclass classification. When working with intrusion detection, the analysis of classification reports showed that the model accurately predicted each class. It describes various metrics such as precision, recall, F1-score, and support for each class. These metrics were calculated as follows:

Accuracy: It assesses the overall correctness of the model.

$$Accuracy = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative} \quad (6)$$

Recall: Recall is a measure of how many of the positive cases the classifier correctly predicted.

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (7)$$

Precision: It is a measure combining both precision and recall

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive} \quad (8)$$

F1-Score: It is a measure combining both precision and recall

$$F1 - Score = 2 * \frac{precision * recall}{precision + recall} \quad (9)$$

Matthews Correlation Coefficient (MCC): This advanced metric is used to measure the quality of both classification, even when the classes are imbalanced.

$$MCC = \frac{c \cdot s - \sum_k p_k t_k}{\sqrt{(s^2 - \sum_k p_k^2)(s^2 - \sum_k t_k^2)}} \quad (10)$$

Cohen's Kappa: This measure is used to evaluate the consistency of the classifier model and adjust for chance agreement.

$$\kappa = \frac{p_o - p_e}{1 - p_e} \quad (11)$$

Adversarial Robustness Score (ARS): This metric assesses a model's stability and its ability to classify attacks robustly.

$$ARS = 1 - \frac{1}{n}\sum_{i=1}^{n} \delta(x_i, x_i^{adv}) \quad (12)$$

Figure 12 shows the binary classification report for the IoT healthcare security 2021 dataset, demonstrating how the suggested model classified the classes more precisely.

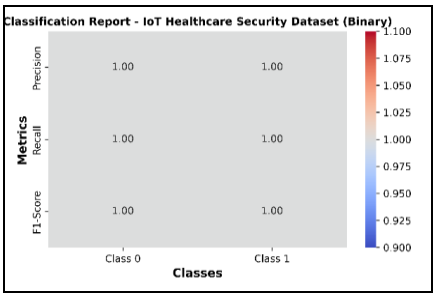

Figure 12. Classification report- IoT healthcare security Dataset

Figure 13 illustrates the high-precision metrics of the proposed model when tested with the WUSTL-EHMS 2020 dataset in both binary and multiclass classification tasks. Although the model exhibited excellent performance across all datasets, it encountered difficulties in classifying data from the CIC IoMT 2024 dataset (Figure 14). The model exhibited overall proficiency and high accuracy, particularly for classes 1 and 2. However, a low precision rate was observed for class 5.

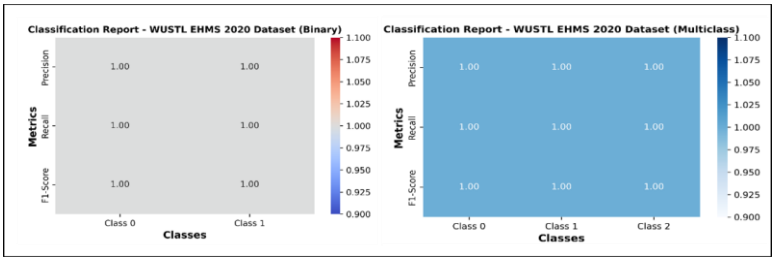

Figure 13. Classification report- WUSTL EHMS 2020 Dataset

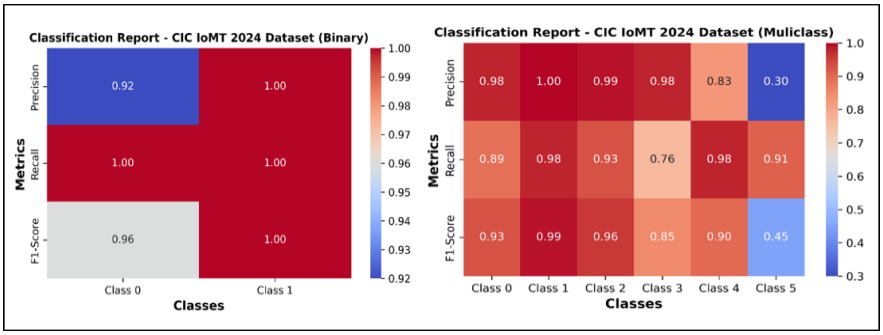

Figure 14. Classification report - CIC IoMT 2024 Dataset

Table 3 shows the binary and multiclass classification results of the proposed model on three datasets along with the average values of various metrics such as accuracy, precision, recall, F1-score, false detection rate (FDR), positive prediction rate (PPR), and area under the curve (AUC) along with advanced metrics to ensure the model robustness and correctness and its agreement between attack and normal classes. These performance metrics indicated that the model demonstrated excellent performance, with no misclassification, in both the WUSTL-EHMS 2020 and IoT Healthcare Security 2021 datasets, for both binary and multiclass classification. The model achieved excellent results on the CIC IoMT binary classification, with an accuracy of 99.8% a minimal FDR of 0.079%. However, the model yielded only somewhat satisfactory performance in multiclass classification, with an accuracy of 90.67%, a precision of 92.89%, a

recall of 90.67% and an F1-score of 91.04%. However, these results are effective for multiclass classification with five attack categories and benign data with a total of 2,068,848 instances.

Table 3. Overall average performance metrics

Dataset (Classification)	Accuracy	Precision	Recall	F1-Score	FDR	PPR	AUC	MCC	Cohen's Kappa	ARS
WUSTL EHMS 2020 (Binary)	1.00	1.00	1.00	1.00	0.00	1.00	1.00	1.00	1.00	1.00
WUSTL EHMS 2020 (Multiclass)	0.99	0.99	0.99	0.99	0.00	0.99	0.99	1.00	1.00	1.00
IoT Healthcare Security (Binary)	1.00	1.00	1.00	1.00	0.00	1.00	1.00	1.00	1.00	1.00
CIC IoMT 2024 (Binary)	0.99	0.99	0.99	0.99	0.079	0.99	0.99	0.95	0.95	0.97
CIC IoMT 2024 (Multiclass)	0.90	0.92	0.90	0.91	0.093	0.90	0.99	0.88	0.88	0.89

4.2. Performance Assessment

The proposed model was evaluated on three different datasets, utilizing both binary and multiclass classifications, and its performance was assessed using various metrics, including accuracy, precision, recall, and F1-score. Table 4 shows that the comprehensive result of the proposed model outperformed the existing models with an accuracy of 99.98%–100.0%, indicating that the model appropriately identified both classes in the WUSTL-EHMS 2020 dataset. While in the IoT healthcare security 2021 dataset, which yielded a more precise classification with performance metrics of 100%. Results of the CIC IoMT 2024 dataset in binary and multiclass classification. The model fitted data well for binary classification with a 99.80% accuracy and 0.079% FDR. During multiclass classification, the performance of the proposed model improved across all metrics compared with the DNN model. Overall, deep learning models, such as autoencoders and LSTMs, outperform various baseline approaches in terms of detection rates, as shown in Table 4. Overall, AUC values range between 0. 99 to 1.0 which shows that the proposed model is a perfect classifier. However, IDS in IoMT requires a high detection rate due to the critical nature of the data related to healthcare, resulting in significant computing expenses. To overcome this, the IDS model should be lightweight and able to outsource computationally demanding tasks to the cloud or servers [51], [52], [53].

Additionally, a key tradeoff exists between real-time processing and batch analysis. Real-time detection is essential for timely detection, but it imposes strict constraints on computation and latency. On the other hand, batch processing is suitable for deeper analysis but delays response, which is not suitable for IoMT as it risks patient safety [54], [55]. Although most IDS models address these critical challenges, integrating IDS into the healthcare domain remains a challenging task that requires significant resources and faces financial limitations [56]. Common challenges include interoperability, ensuring real-time and low latency [34], and compliance with regulations such as HIPAA and GDPR [57].

Table 4. Comparative analysis of proposed system

Model [Reference no]	Dataset	Accuracy	Precision	Recall	F1-Score	FDR	PPR	AUC
DNN –FL[27]	WUSTL EHMS 2020 (Binary)	91.40	65.05	61.42	-	-	-	-
ANN [28]		90.04	-	-	-	-	-	93.42
RCLNet[33]		99.78	99.53	99.83	99.57	-	-	-
LSTM[32]		97.13	96.33	98.28	97.22	-	-	99.30
Proposed model		**1.0**	**1.0**	**1.0**	**1.0**	**0.0**	**1.0**	**1.0**
Stacking [34]	WUSTL EHMS 2020(Multiclass)	98.88	98.23	99.58	98.90	-	-	-
Proposed model		**99.98**	**99.98**	**99.98**	**99.98**	**0.0**	**99.98**	**99.99**
Comparative model of IoT Healthcare security dataset								
RF [30]	IoT Healthcare Security	99.51	99.79	99.70	99.65	-	-	-
LSTM[32]		99.74	99.91	99.46	99.68	-	-	99.94
Proposed model		**1.0**	**1.0**	**1.0**	**1.0**	**0.0**	**1.0**	**1.0**
Comparative model of CIC IoMT 2024 Dataset								
DNN [29]	CIC IoMT 2024 (Binary)	99.61	95.23	96.27	95.74	-	-	-
Proposed model		**99.80**	**99.81**	**99.80**	**99.80**	**0.079**	**99.99**	**99.99**
DNN [29]	CIC IoMT 2024 (Multiclass)	78.05	76.02	76.80	73.35	-	-	-
UNet++ LSTM[31]		87.96	94.55	93.31	86.47	-	-	93.64
Proposed model		**90.67**	**92.89**	**90.67**	**91.04**	**0.093**	**90.67**	**99.98**

Future research on IDS in IoMT focuses on enhancing scalability to handle vast amounts of data in the healthcare domain. As the expansion of healthcare advancements demands high dimensionality, detecting real-time traffic efficiently can be achieved using distributed computing platforms, such as Apache Spark, which enables low latency [58]. Federated IDS and blockchain techniques enables data privacy while maintaining a high detection rate [59] [60], and supports explainable AI for IDS [61].

5. CONCLUSION

IoT systems are used in various domains to collect important data using sensors, boards, and other devices. When important data, such as health and financial information, is transmitted over a network, the risk of cyber threats is involved. In this study, a model was proposed for detecting intrusions in healthcare data. To this end, the importance and challenges involved in the security of IoMT infrastructure were evaluated. The proposed model consisted of three layers: a data layer for data preprocessing and cleaning, a semantic layer for feature representation as a weighted knowledge graph using a sparse autoencoder, and a detection layer for intrusion detection, utilizing a combined model of a deep autoencoder with LSTM and XGBoost for attack likelihood analysis. The performance of the model was assessed by applying it to three real-time datasets: WUSTL-EHMS 2020, IoT Healthcare Security 2021, and CIC IoMT 2024. This served as the foundation for addressing intrusion detection in healthcare IoT systems. These datasets contained various simulated and real-time attacks, including spoofing, data alteration, DDoS, DoS, and MQTT attacks, as well as other common attacks in IoMT devices. The model's performance was comprehensively evaluated. The suggested model performed exceptionally well, with a high detection rate, minimal loss, and a low FDR in both binary and multiclass classification in the WUSTL-EHMS 2020 and IoT Healthcare Security 2021 datasets, as well as in the binary classification of CIC IoT 2024. However, it only performed satisfactorily on the CIC IoMT 2024 dataset multiclass classification with five attack categories. In the future, the model will be

evaluated in real-time to detect intrusions, and an autonomous lightweight IDS will be created. It is also intended to scale the model to accommodate large datasets.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the RUSA-Phase II (Rashtriya Uchchatar Shiksha Abiyan, Ref -016/RUSA/MKU/2020-2021), Department of Computer Science, School of Information Technology, Madurai Kamaraj University, Madurai- 625021 for their financial support.

REFERENCES

[1] S. E. El-deep, A. A. Abohany, K. M. Sallam, and A. A. A. El-Mageed, "A comprehensive survey on impact of applying various technologies on the internet of medical things," *Artif. Intell. Rev.*, vol. 58, no. 3, p. 86, Jan. 2025, doi: 10.1007/s10462-024-11063-z.

[2] B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends," *Sustain.*, vol. 15, no. 7, p. 6177, Apr. 2023, doi: 10.3390/su15076177.

[3] T. Dutta, S. Pramanik, and P. Kumar, "IoT for healthcare industries: A tale of revolution," in *Healthcare Paradigms in the Internet of Things Ecosystem*, Elsevier, 2020, pp. 21–45. doi: 10.1016/B978-0-12-819664-9.00002-8.

[4] A. Jha, A. Athanerey, and A. Kumar, "Role and challenges of internet of things and informatics in Healthcare research," *Health Technol. (Berl).*, vol. 12, no. 4, pp. 701–712, Jul. 2022, doi: 10.1007/s12553-022-00661-y.

[5] Cynerio, "Cynerio report 2022 & 2023." [Online]. Available: Www.Cynerio.Com

[6] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: How safe are we?," *BMJ*, vol. 358, p. j3179, Jul. 2017, doi: 10.1136/bmj.j3179.

[7] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, no. March, pp. 48–52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.

[8] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[9] M. M. Ozcelik, I. Kok, and S. Ozdemir, "A Survey on Internet of Medical Things (IoMT): Enabling Technologies, Security and Explainability Issues, Challenges, and Future Directions," *Expert Syst.*, vol. 42, no. 5, May 2025, doi: 10.1111/exsy.70010.

[10] S. Ryu, "Book Review: mHealth: New Horizons for Health through Mobile Technologies: Based on the Findings of the Second Global Survey on eHealth (Global Observatory for eHealth Series, Volume 3)," *Healthc. Inform. Res.*, vol. 18, no. 3, p. 231, 2012, doi: 10.4258/hir.2012.18.3.231.

[11] R. Hireche, H. Mansouri, and A. S. K. Pathan, "Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis," *J. Cybersecurity Priv.*, vol. 2, no. 3, pp. 640–661, Aug. 2022, doi: 10.3390/jcp2030033.

[12] Meggitt S., "MEDJACK Attacks: The Scariest Part of the Hospital," *Tufts Univ.*, 2018, [Online]. Available: https://www.cs.tufts.edu/comp/116/archive/fall2018/smeggitt.pdf

[13] D. Halperin *et al.*, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proceedings - IEEE Symposium on Security and Privacy*, IEEE, May 2008, pp. 129–142. doi: 10.1109/SP.2008.31.

[14] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Comput. Secur.*, vol. 86, pp. 147–167, Sep. 2019, doi: 10.1016/j.cose.2019.06.005.

[15] M. Akshay Kumaar, D. Samiayya, P. M. D. R. Vincent, K. Srinivasan, C. Y. Chang, and H. Ganesh,

"A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning," *Front. Public Heal.*, vol. 9, Jan. 2022, doi: 10.3389/fpubh.2021.824898.

[16] S. Roy, J. Li, B. J. Choi, and Y. Bai, "A lightweight supervised intrusion detection mechanism for IoT networks," *Futur. Gener. Comput. Syst.*, vol. 127, pp. 276–285, Feb. 2022, doi: 10.1016/j.future.2021.09.027.

[17] A. Alferaidi *et al.*, "Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles," *Math. Probl. Eng.*, vol. 2022, pp. 1–8, Mar. 2022, doi: 10.1155/2022/3424819.

[18] A. Raghuvanshi *et al.*, "Intrusion Detection Using Machine Learning for Risk Mitigation in IoT-Enabled Smart Irrigation in Smart Farming," *J. Food Qual.*, vol. 2022, pp. 1–8, Feb. 2022, doi: 10.1155/2022/3955514.

[19] C. Iwendi, J. H. Anajemba, C. Biamba, and D. Ngabo, "Security of things intrusion detection system for smart healthcare," *Electron.*, vol. 10, no. 12, p. 1375, Jun. 2021, doi: 10.3390/electronics10121375.

[20] M. Bakro *et al.*, "Efficient Intrusion Detection System in the Cloud Using Fusion Feature Selection Approaches and an Ensemble Classifier," *Electron.*, vol. 12, no. 11, p. 2427, May 2023, doi: 10.3390/electronics12112427.

[21] T. Öztürk, Z. Turgut, G. Akgün, and C. Köse, "Machine learning-based intrusion detection for SCADA systems in healthcare," *Netw. Model. Anal. Heal. Informatics Bioinforma.*, vol. 11, no. 1, p. 47, Dec. 2022, doi: 10.1007/s13721-022-00390-2.

[22] A. Verma and V. Ranga, "Machine Learning Based Intrusion Detection Systems for IoT Applications," *Wirel. Pers. Commun.*, vol. 111, no. 4, pp. 2287–2310, Apr. 2020, doi: 10.1007/s11277-019-06986-8.

[23] A. John, I. F. Bin Isnin, S. H. H. Madni, and M. Faheem, "Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms," *Intell. Syst. with Appl.*, vol. 22, p. 200381, Jun. 2024, doi: 10.1016/j.iswa.2024.200381.

[24] P. G. Shambharkar and N. Sharma, "Deep learning-empowered intrusion detection framework for the Internet of Medical Things environment," *Knowl. Inf. Syst.*, vol. 66, no. 10, pp. 6001–6050, Oct. 2024, doi: 10.1007/s10115-024-02149-9.

[25] M. Zubair *et al.*, "Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System †," *Sensors*, vol. 22, no. 21, p. 8280, Oct. 2022, doi: 10.3390/s22218280.

[26] N. Goswami *et al.*, "Preserving Security in Internet of Things Healthcare System with Metaheuristic Driven Intrusion Detection," *Eng. Sci.*, vol. 25, Oct. 2023, doi: 10.30919/es933.

[27] F. Mosaiyebzadeh, S. Pouriyeh, R. M. Parizi, M. Han, and D. M. Batista, "Intrusion Detection System for IoHT Devices using Federated Learning," in *IEEE INFOCOM 2023 - Conference on Computer Communications Workshops, INFOCOM WKSHPS 2023*, IEEE, May 2023, pp. 1–6. doi: 10.1109/INFOCOMWKSHPS57453.2023.10225932.

[28] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," *IEEE Access*, vol. 8, pp. 106576–106584, 2020, doi: 10.1109/ACCESS.2020.3000421.

[29] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, and A. A. Ghorbani, "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT," *Internet of Things (Netherlands)*, vol. 28, p. 101351, Dec. 2024, doi: 10.1016/j.iot.2024.101351.

[30] F. Hussain *et al.*, "A framework for malicious traffic detection in iot healthcare environment," *Sensors*, vol. 21, no. 9, p. 3025, Apr. 2021, doi: 10.3390/s21093025.

[31] A. Mezina, J. Nurmi, and S. Member, "Novel Hybrid UNet ++ and LSTM Model for Enhanced Attack Detection and Classification in IoMT Traffic," *IEEE Access*, vol. PP, p. 1, 2025, doi: 10.1109/ACCESS.2025.3553966.

[32] M. Benmalek, A. Seddiki, and K. Haouam, "SNN-IoMT : A Novel AI-Driven Model for Intrusion Detection in Internet of," 2025, doi: http://dx.doi.org/10.32604/cmes.2025.062841.

[33] J. A. Shaikh *et al.*, "RCLNet: an effective anomaly-based intrusion detection for securing the IoMT system," *Front. Digit. Heal.*, vol. 6, Oct. 2024, doi: 10.3389/fdgth.2024.1467241.

[34] T. Alsolami, B. Alsharif, and M. Ilyas, "Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical Things," *Sensors*, vol. 24, no. 18, p. 5937, Sep. 2024, doi: 10.3390/s24185937.

[35] A. Ghourabi, "A Security Model Based on LightGBM and Transformer to Protect Healthcare

Systems From Cyberattacks," *IEEE Access*, vol. 10, pp. 48890–48903, 2022, doi: 10.1109/ACCESS.2022.3172432.

[36] M. Hofer, D. Obraczka, A. Saeedi, H. Köpcke, and E. Rahm, "Construction of Knowledge Graphs: Current State and Challenges," Aug. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/info15080509.

[37] B. Chen, H. Li, D. Zhao, Y. Yang, and C. Pan, "Quality assessment of cyber threat intelligence knowledge graph based on adaptive joining of embedding model," *Complex Intell. Syst.*, vol. 11, no. 1, Jan. 2025, doi: 10.1007/s40747-024-01661-3.

[38] H. Li, Z. Shi, C. Pan, D. Zhao, and N. Sun, "Cybersecurity knowledge graphs construction and quality assessment," *Complex Intell. Syst.*, vol. 10, no. 1, pp. 1201–1217, Feb. 2024, doi: 10.1007/s40747-023-01205-1.

[39] I. Sarhan and M. Spruit, "Open-CyKG: An Open Cyber Threat Intelligence Knowledge Graph," *Knowledge-Based Syst.*, vol. 233, p. 107524, Dec. 2021, doi: 10.1016/j.knosys.2021.107524.

[40] E. Gilliard, J. Liu, and A. A. Aliyu, "Knowledge graph reasoning for cyber attack detection," *IET Commun.*, vol. 18, no. 4, pp. 297–308, Mar. 2024, doi: 10.1049/cmu2.12736.

[41] X. Hao *et al.*, "Construction and application of a knowledge graph," *Remote Sens.*, vol. 13, no. 13, p. 2511, Jun. 2021, doi: 10.3390/rs13132511.

[42] A. Harnoune, M. Rhanoui, M. Mikram, S. Yousfi, Z. Elkaimbillah, and B. El Asri, "BERT based clinical knowledge extraction for biomedical knowledge graph construction and analysis," *Comput. Methods Programs Biomed. Updat.*, vol. 1, p. 100042, Jan. 2021, doi: 10.1016/j.cmpbup.2021.100042.

[43] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, "1999 DARPA off-line intrusion detection evaluation," *Comput. Networks*, vol. 34, no. 4, pp. 579–595, Oct. 2000, doi: 10.1016/S1389-1286(00)00139-0.

[44] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009*, IEEE, Jul. 2009, pp. 1–6. doi: 10.1109/CISDA.2009.5356528.

[45] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*, IEEE, Nov. 2015, pp. 1–6. doi: 10.1109/MilCIS.2015.7348942.

[46] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, SCITEPRESS - Science and Technology Publications, 2018, pp. 108–116. doi: 10.5220/0006639801080116.

[47] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," *J. Sensors*, vol. 2016, pp. 1–16, 2016, doi: 10.1155/2016/4731953.

[48] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Futur. Gener. Comput. Syst.*, vol. 100, pp. 779–796, Nov. 2019, doi: 10.1016/j.future.2019.05.041.

[49] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and Adna N Anwar, "TON-IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020, doi: 10.1109/ACCESS.2020.3022862.

[50] A. Razavi, S. Mahdavifar, N. Maleki, A. H. Lashkari, and M. Broda, (2021) "Classifying Malicious Domains using DNS Traffic Analysis". doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech52372.2021.00024.

[51] G. Zhao, Y. Wang, and J. Wang, "Lightweight Intrusion Detection Model of the Internet of Things with Hybrid Cloud-Fog Computing," *Secur. Commun. Networks*, vol. 2023, pp. 1–16, Jan. 2023, doi: 10.1155/2023/7107663.

[52] A. Salehpour, M. A. Balafar, and A. Souri, "An optimized intrusion detection system for resource-constrained IoMT environments: enhancing security through efficient feature selection and classification," *J. Supercomput.*, vol. 81, no. 6, p. 783, Apr. 2025, doi: 10.1007/s11227-025-07253-3.

[53] Nguyen, Son & Dung, Ha. (2023). A Lightweight Method for Detecting Cyber Attacks in High-traffic Large Networks based on Clustering Techniques. International journal of Computer Networks & Communications. 15. 35-51. 10.5121/ijcnc.2023.15103.

[54] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," in *2018 IEEE Security and Privacy Workshops (SPW)*, IEEE, May 2018, pp. 29–35. doi: 10.1109/SPW.2018.00013.

[55] K. S. Adewole *et al.*, "Empirical Analysis of Data Streaming and Batch Learning Models for Network Intrusion Detection," *Electronics*, vol. 11, no. 19, p. 3109, Sep. 2022, doi: 10.3390/electronics11193109.

[56] J. Elhachmi and A. Kobbane, "Blockchain-based security mechanisms for Internet of Medical Things (IoMT)," *Int. J. Comput. Netw. Commun. (IJCNC)*, vol. 14, pp. 115–136, 2022, doi: 10.5121/ijcnc.2022.14608.

[57] A. Yazid, "Cybersecurity and privacy issues in the internet of medical things (IoMT)," *Eig. Rev. Sci. Technol.*, vol. 7, no. 1, pp. 1–21, 2023.

[58] E. Alalwany, B. Alsharif, Y. Alotaibi, A. Alfahaid, I. Mahgoub, and M. Ilyas, "Stacking Ensemble Deep Learning for Real-Time Intrusion Detection in IoMT Environments," *Sensors*, vol. 25, no. 3, p. 624, Jan. 2025, doi: 10.3390/s25030624.

[59] K. Begum, M. A. I. Mozumder, M. Il Joo, and H. C. Kim, "BFLIDS: Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks," *Sensors*, vol. 24, no. 14, p. 4591, Jul. 2024, doi: 10.3390/s24144591.

[60] V. Hariharasudhan and Vetrivelan, P. (2023). Blockchain-Based Secure and Scalable Routing Mechanisms for VANETs Applications. International journal of Computer Networks & Communications. 15. 129-148. , doi: 10.5121/ijcnc.2023.15308.

[61] A. Si-ahmed, M. A. Al-Garadi, and N. Boustia, "Explainable Machine Learning-Based Security and Privacy Protection Framework for Internet of Medical Things Systems," 2024, doi: 10.48550/arXiv.2403.09752.

AUTHORS

Ms. V.G. Aishvaryashree is a research scholar at the Department of Computer Science, School of Information Technology, Madurai Kamaraj University, India. She received the Bachelor of Computer Applications from Madurai Kamaraj University, Madurai in 2018 and the Master of Computer Applications degree from the Anna University. She is currently pursuing a Ph.D. in Computer Science at Madurai Kamaraj University. Her research interests include cybersecurity, recommender systems, and AI.

Dr. M Thangaraj is currently the Professor and Head of the Computer Science Department at Madurai Kamaraj University, India, He has rich academic background, obtained his post-graduate degree in Computer Science from Alagappa University, Karaikudi; M.Tech. in Computer Science from Pondicherry University, and a Ph.D. degree in Computer Science from Madurai Kamaraj University, Tamil Nadu, in 2006. He is an active researcher, focuses on Big Data, Social Media Analytics, and Wireless Sensor Networks. His extensive research contributions are evident in his publication of over 150 papers in journals and conference proceedings.

Dr. M. Nirmala Devi is a Life member in ISTE and she is serving as Assistant Professor (Selection Grade) in the Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, Tamil Nadu, India. She completed her Ph.D. at Anna University Chennai in 2019. She has 19 years of teaching and research experience with 52 publications on IEEE, Springer, CRC, Taylor and Francis and IGI Global. She has 159 Google Scholar and 105 Scopus citations. Her publications are in the areas of Data Science and Analysis, Deep Learning, AI, ML and Design Thinking for Healthcare, Agriculture, and pedagogical domain. She bagged Proficiency and Mentoring Awards from IBM, Infosys, IITB, NPTEL and Smart India Hackathon.