INTRUSION DETECTION SYSTEM FOR INTERNET OF MEDICAL THINGS USING GRU WITH ATTENTION MECHANISM-BASED HYBRID DEEP LEARNING TECHNIQUE

Naveen Saran and Nishtha Kesswani

(Received: 6-Sep.-2024, Revised: 8-Nov.-2024, Accepted: 21-Nov.-2024)

ABSTRACT

The proliferation of Internet of Things devices in healthcare, specifically the Internet of Medical Things, has revolutionized patient care and health-monitoring systems. Integrating these interconnected medical devices introduces unprecedented security challenges, necessitating robust Intrusion Detection Systems (IDSs) to safeguard patient data and healthcare infrastructure. To protect the IoMT devices from numerous malicious attacks, researchers have developed numerous Intrusion Detection Systems, but the development of an effective and real-time IDS remains a challenge. Our proposed IDS addresses this gap and surpasses state-of-the-art IDS techniques for IoMT networks. In this research paper, we have proposed a novel IDS approach for IoMT, leveraging a Hybrid Deep Learning technique to enhance detection accuracy and efficiency. By combining the strengths of Gated Recurrent Unit (GRU) and Attention Mechanism, the proposed IDS achieves superior performance in detecting anomalous activities in medical networks. We evaluated the proposed IDS model on two publicly available benchmark intrusion datasets and achieved 99.99 % accuracy on the ICU Healthcare Dataset and 98.94 % on the NF-TON-IoT Dataset. Precision, Recall, F1-score metrics and ROC-AUC for the proposed model are promising. We also added Noise to the features to show how effectively the model performed in noisy environments. Moreover, we used the K-Fold Cross Validation Technique to cross-validate the model's performance on both datasets, ensuring the reliability and applicability of the suggested IDS model for IoMT networks.

KEYWORDS

Internet of medical things, Intrusion-detection system, Principal-component analysis, Deep learning, Gated recurrent unit, Attention mechanism, K-fold cross validation.

1. INTRODUCTION

The Internet of Things (IoT) innovation has changed various industries, such as health care. 560M wearable are expected to ship by 2024, which will track and visualize real-time healthcare data [1] and this number could increase. The Internet of Medical Things (IoMT) has introduced several devices, including wearable health monitors, implantable medical devices and smart hospital equipment, that have brought a revolution in the way patients are treated, diagnosed and cared for by enabling remote monitoring, real-time health tracking, personalized medicine [2] and ultimately become an integral part of Smart Healthcare Systems. However, the widespread adoption of IoMT devices has introduced unprecedented security challenges, particularly concerning the protection of sensitive patient data produced by these Internet of Medical Things (IoMT) apps for remote healthcare monitoring from vital signs and other signals like Electro-Cardio-Gram (ECG) and Electro-Encephalo-Gram (EEG) and the integrity of healthcare infrastructure. Nonetheless, instances of cyber-attacks targeting sensitive medical information present a severe risk. The aim is to protect health data against multiple intrusion attacks [3]. Thus, an attacker tampering with this data can cause severe medical problems, including misdiagnosis, thereby resulting in delays in emergency care or causing death [4]. Consequently, the research examines the safety of IoMT-generated health data from the perspective of Smart Healthcare Systems.

Attackers can remotely control IoMT devices to build IoT-based botnets, since they are simple to hack and attack. These assaults result in violations, infringements and disclosures of sensitive data inside the wider IoT-enabled system. Common attacks on Internet of Things (IoT)-based healthcare devices

N. Saran is with Department of Computer Science and N. Kesswani is with Department of Data Science & Analytics, Central University of Rajasthan, Bandarsindri, Kishangarh, Ajmer, Rajasthan, India. Emails: naveen.saran90@gmail.com and nishtha@curaj.ac.in

include denial-of-service (DOS), ransomware, distributed denial-of-service (DDoS) and botnet attacks [5]. Figure 1 illustrates the cyber-attacks on IoMT network communication targeting vulnerable sensor devices towards known, unknown and zero-day intrusion attacks by intruders. The inter-connectivity of these devices, coupled with their susceptibility to cyber-threats, significantly expose patients' data safety.

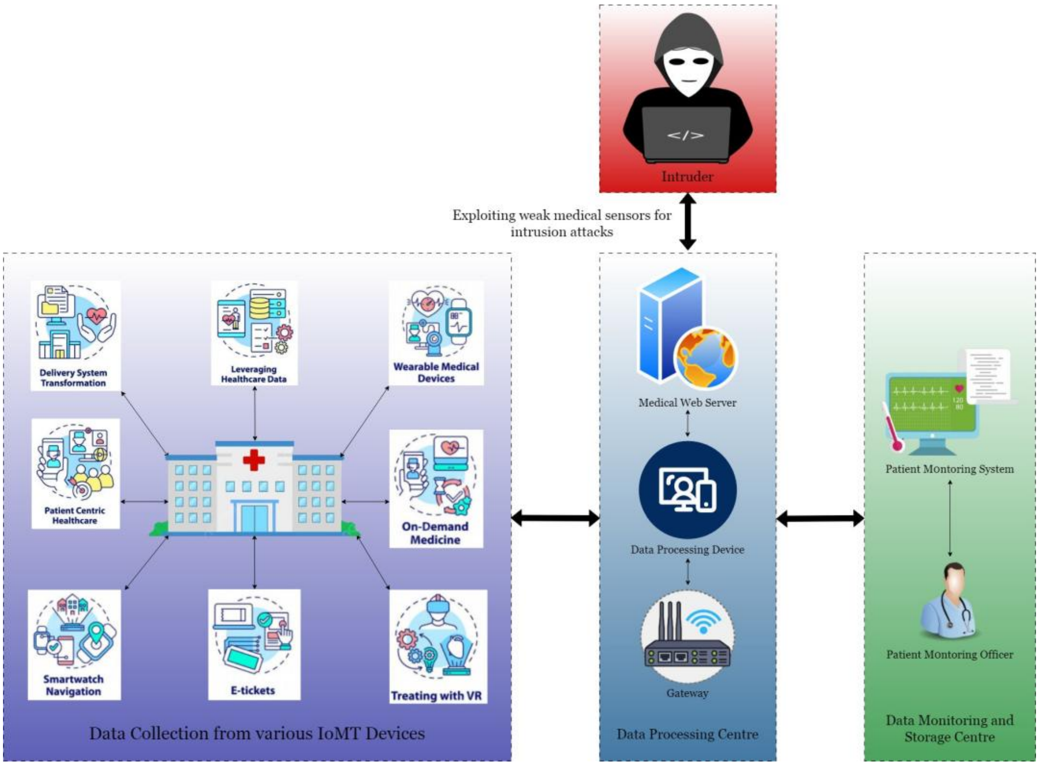
Intruder
</>
Exploiting weak medical sensors for intrusion attacks
Delivery System Transformation
Leveraging Healthcare Data
Wearable Medical Devices
Patient Centric Healthcare
On-Demand Medicine
Smartwatch Navigation
E-tickets
Treating with VR
Data Collection from various IoMT Devices
Medical Web Server
Data Processing Device
Gateway
Data Processing Centre
Patient Montoring System
Patient Montoring Officer
Data Monitoring and Storage Centre

Figure 1. Internet of medical things vulnerability and attacks.

To address such emerging cyber-threats, there has been a need for robust Intrusion Detection Systems (IDSs) specifically designed for the Internet of Medical Things [6]-[8]. An IDS acts as the primary defence line against cyber-attacks by continuously monitoring network traffic, identifying any abnormal activity and alerting healthcare providers about possible security breaches instantly. However, traditional IDS solutions may not be suitable in an IoMT environment due to their unique nature where resources are limited, devices have different architectures and they operate dynamically [9]. To address these challenges, this research proposes a novel approach for intrusion detection in IoMT, leveraging a Hybrid Deep Learning technique to enhance detection accuracy and efficiency. The novelty of the proposed approach is the integration of a Gated Recurrent Unit (GRU) with an Attention Mechanism for Intrusion Detection and Classification and Principal Component Analysis (PCA) for Feature Engineering. The proposed Intrusion Detection System (IDS) seeks to offer all-encompassing coverage of anomalous behaviors and cyber-threats within medical networks. Also, we have used K-Fold Cross-validation procedures, which assess the model's performance on every fold, to ensure the model's robustness.

This paper presents a detailed analysis of the proposed IDS architecture, its implementation and its performance evaluation using real-time scenario-based publicly available benchmark datasets like ICU Healthcare Dataset and NF-TON-IoT Dataset. In summary, this research contributes to advancing security in healthcare by developing a specialized IDS solution tailored for the Internet of Medical Things. By leveraging the power of hybrid Deep Learning techniques, the proposed IDS offers enhanced known, unknown and zero-day intrusion attack-detection capabilities in real-time scenarios, safeguarding patient data and ensuring the integrity of IoMT infrastructure. The main contributions of this paper are as follows:

- **Comprehensive Data Pre-processing:** This has been achieved by standardizing numerical features, reducing Dimensions using PCA and handling class imbalance with SMOTE.

- **GRU with Attention Mechanism:** The incorporation of a custom attention layer captures temporal dependencies and important features.
- **Hyper-parameter Tuning:** This has been carried out using keras-tuner to optimize model parameters.
- **Robust Model Training:** This has been ensured by early stopping to prevent over-fitting.
- **Robustness to Noise:** The model performance has been evaluated with added noise.
- **Cross-validation (CV) for Stability:** A stratified K-Fold CV was carried out for stability assessment.
- **Scalability and Real-time Potential:** The proposed model is designed for real-time intrusion-detection scenarios and the scalable architecture is adaptable to new threats.

Our research presents an innovative approach to enhancing Intrusion-detection Systems for the Internet of Medical Things by implementing a sophisticated GRU model with an attention mechanism. This advanced architecture effectively captures temporal dependencies and highlights significant features in IoMT data, improving the detection of intricate cyber-attacks. Comprehensive data pre-processing steps, including standardization, dimensionality reduction using PCA and handling class imbalance with SMOTE, ensure the model's effectiveness. Hyper-parameter tuning using a keras-tuner optimizes model parameters and early stopping prevents over-fitting during robust model training. We tackle the issue of imbalanced data by utilizing the Synthetic Minority Over-sampling Technique (SMOTE) and ensure the model's robustness through K-Fold Cross-validation. Our IDS is designed for real-time processing, enabling swift detection and response to emerging threats. It offers high scalability and adaptability, accommodating new threats and processing diverse IoMT data. The model's robustness to noise is verified by evaluating performance with added noise. Evaluated on comprehensive ICU Healthcare and NF-TON-IoT Datasets, our model accurately identifies known and novel attacks, significantly enhancing security in real-time IoMT environments. Our evaluation results demonstrate that this proposed method outperforms existing techniques, which lack these advanced capabilities.

The rest of the research article is organized as follows: The paper's second section discusses the related research works based on machine-learning and deep-learning techniques used to implement the IDS model for the IoMT network. The third section discusses the preliminary concepts used in the proposed IDS model. The fourth section consists of the proposed research methodology. The fifth section contains complete information about the experimental setting required to operate and build an effective IDS model for IoMT. The sixth section comprises the experimental results and a detailed analytical report of our proposed IDS model. At last, section seven discusses the conclusion and the future scope of the proposed research work.

2. RELATED WORKS

In this work, we analyze the literature on intrusion detection in the Internet of Medical Things networks, focusing on applying various Machine Learning (ML) and Deep Learning(DL) techniques researchers employ to develop their respective IDS models. We explore the use of traditional ML algorithms such as Decision Trees (DTs) [10], Random Forests (RFs) and Ensemble Learning (EL) [11] for anomaly detection and classification tasks in IoMT networks. Additionally, we examine advanced DL approaches, including Convolutional Neural Networks (CNNs) [12], Recurrent Neural Networks (RNNs) [13] and others that offer data-driven and automated solutions for identifying complex patterns and anomalies in network-traffic data. Through this comprehensive review, we aim to highlight the strengths and drawbacks of ML and DL approaches in the context of IoMT, providing insights into their efficacy, scalability and adaptability to evolving cyber-threats in healthcare environments. Tables 1 and 2 emphasize the critical facts of state-of-the-art machine-learning and deep-learning Techniques proposed by researchers to construct an IDS model for IoMT networks.

2.1 Machine Learning-based IDS for IoMT

Using a fog-cloud-based architecture, Kumaret al. [14] suggested Ensemble Learning (EL) based IDS for IoMT environments. To identify attackers in the edge-centric IoMT framework, Nandy et al. [15] suggested an Empirical Intelligent Agent (EIA) based on a novel Swarm-Neural Network (Swarm-NN) technique. To secure the data of IoMT applications, Singh et al. [16] presented a Dew-Cloud-based model employing Hierarchical Federated Learning (HFL). Wagan et al. [17] described the Duo-Secure IoMT framework, which distinguishes between routine IoMT data and attack patterns using multi-modal sensory signals data. Khan et al. [18] examined the suggested technique for IoMT cyber-attacks by employing ensemble- based techniques and fog-cloud infrastructure. Using a meta-learning strategy, Zukaib et al. [19] developed a Meta-IDS model that improves the detection of known and zero-day intrusions in the IoMT environment.

Table 1. State-of-the-art machine-learning techniques.

References	Methodology	Dataset	Accuracy	Limitations
Kumar et al. [14]	Ensemble learning using fog-cloud architecture.	TON-IoT	96.35%	To detect intrusions in IoMT networks, the suggested model is not sufficiently compared in the paper to other cutting-edge ensemble or DL models.
Nandy et al. [15]	Using a Swarm-Neural Network approach based on Empirical Intelligent Agents (EIAs) to detect threats and evaluate the effectiveness of health data.	TON-IoT	99.50%	The paper does not compare the proposed Swarm-NN approach and existing intrusion-detection techniques in the IoMT frameworks.
Singh et al. [16]	For data privacy in IoMT, the Hierarchical Long- Short Term Memory model is implemented at dispersed Dew servers with a cloud computing-supported backend.	TON-IoT	99.31%	The paper's comparison of the HFL-HLSTM model with existing intrusion-detection techniques is limited.
Wagan et al. [17]	Dynamic Fuzzy C-Means clustering with Bi-LSTM technique to identify attack patterns within the IoMT network.	WUSTL EHMS 2020	89.67%	Dataset holds very few records.
Khan et al. [18]	Fog-cloud architecture and Ensemble Learning to handle IoMT security concerns.	TON-IoT	98.56%	The paper fails to identify emerging or unknown attacks in future IoMT environments.

Table 2. State-of-the-art deep-learning techniques.

References	Methodology	Dataset	Accuracy	Limitations
RM et al. [20]	PCA with Grey-wolf Optimization for feature engineering and DNN for attack classification.	KDD99, UNSW-B15	99.99%, 89.13%	Lacks real-time implementation in live IoMT environment with sensitive medical data.
Khan et al. [21]	SDN enabled hybrid deep learning-based IDS for IoMT.	IoT	99.83%	The paper lacks a comprehensive comparison with other state-of-the-art malware-detection methods on the same dataset.
Awotunde et al. [22]	Swarm-Neural Network-based IDS model for IoMT devices.	NF-TON-IoT	89.00%	The paper fails to specify which existing models or techniques were used to compare the proposed model's performance on the same dataset.
Saran et al. [23]	S-RNN, LSTM and GRU-based deep-learning technique to build IDS model for IoMT devices.	ICU Healthcare	99.00%	The paper fails to handle imbalanced datasets and model's robustness in noisy conditions.
Saheed et al. [24]	Deep Recurrent Neural Networks and Supervised machine-learning models were used to develop an IDS for IoMT environment.	NSL-KDD	99.76%	The dataset lacks the latest real-world IoMT attacks and traffic.
Changanti et al. [25]	PSO with DNN is used to implement an effective and accurate IDS in IoMT.	WUSTLE HMS 2020	96.00%	Dataset holds very few records.
Alzubi et al. [26]	Blended DL framework leveraging the CNN-LSTM to recognize the latest intrusion attacks and defend the healthcare data.	CIC-IDS 2018	98.53%	Data imbalance and bias-mitigation strategies are not investigated.

2.2 Deep-learning Techniques for IDS in IoMT

An IDS based on Deep Neural Networks (DNNs) was proposed by RM et al. [20] to identify and anticipate unknown threats in an IoMT context. Using a combination of CNN and LSTM techniques, Khan et al. [21] provided an SDN-enabled hybrid Deep Learning-based IDS for IoMT. To identify intrusions in the data-centric IoMT system, Awotunde et al. [22] proposed a Swarm-Neural Network-based intrusion detection system (IDS) model. Saran et al. [23] discussed S-RNN, LSTM and GRU-based Deep-learning Techniques to identify intrusion attacks in the IoMT environment. In Saheed et al. [24], it was shown how an efficient and effective IDS for classifying and forecasting unforeseen cyber-threats in the IoMT environment can be developed using a Deep Recurrent Neural Network (DRNN) and Supervised Machine Learning (SML) models (Random Forest, Decision Tree, KNN and Ridge Classifier). To enhance the performance of IDS in IoMT, Changanti et al. [25] introduced the DNN-based DL model and the PSO feature-selection technique. Alzubi et al. [26] presented a hybrid deep-learning framework that combines the advantages of Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) to effectively detect the most recent intrusion attacks and safeguard medical data.

3. PRELIMINARIES

Preliminary concepts that are used to build a robust, secure and effective IDS solution are discussed in the following sub-section.

3.1 Gated Recurrent Unit (GRU) with Attention Mechanism

By enabling the model to focus on the most essential parts of the input sequence during prediction, the integration of an Attention Mechanism [27] with a Gated Recurrent Unit (GRU) [28] enhances the performance of the GRU. Unlike the general LSTM, CNN and GRU hybrid techniques, this technique efficiently prioritises essential temporal dependencies for the model, leading to enhanced accuracy in various IoT/IoMT applications. The GRU effectively prevents information loss by using update and reset gates to regulate information flow and refresh the hidden state. To determine what information should be prioritized, the Attention Mechanism computes a context vector by adding the weighted total of the hidden states. Alignment scores are used to calculate the hidden-state weights. By combining these two methods, the model's capacity to manage long-range dependencies in sequential data is greatly enhanced, which makes it very helpful for complicated-pattern identification in IoMT contexts. The core equations for the GRU with Attention Mechanism are as follows:

GRU Equations:

$$\mathrm{z}_t = \sigma(\mathrm{W}_z \mathrm{x}_t + \mathrm{U}_z \mathrm{h}_{t-1} + \mathrm{b}_z) \tag{1}$$

$$\mathrm{r}_t = \sigma(\mathrm{W}_r \mathrm{x}_t + \mathrm{U}_r \mathrm{h}_{t-1} + \mathrm{b}_r) \tag{2}$$

$$\tilde{\mathrm{h}}_{\boldsymbol{t}} = \tanh(\mathrm{W}_h \mathrm{x}_t + \mathrm{U}_h(\mathrm{r}_t \odot \mathrm{h}_{t-1}) + \mathrm{b}_h) \tag{3}$$

$$\mathrm{h}_t = (1 - \mathrm{z}_t) \odot \mathrm{h}_{t-1} + \mathrm{z}_t \odot \tilde{\mathrm{h}}_{\boldsymbol{t}} \tag{4}$$

where x_t is the input, zt is the update gate, r_t is the reset gate, $\mathrm{h}\tilde{}_t$ is the candidate's hidden state and h_t is the hidden state at time step *t*. The functions σ and tanh represent the sigmoid and hyperbolic tangent activation functions, respectively. ⨀ is the element-wise multiplication function [29].

Attention-mechanism Equations:

$$\boldsymbol{e_{t,i}} = \mathrm{v}^{\top} \mathbf{tanh}(\mathbf{W}_{\boldsymbol{e}} \boldsymbol{h_t} + \mathbf{U}_{\boldsymbol{e}} \mathbf{h}_{\boldsymbol{i}} + \mathbf{b}_{\boldsymbol{e}}) \tag{5}$$

$$\boldsymbol{\alpha_{t,i}} = \frac{\mathbf{exp}(\boldsymbol{e_{t,i}})}{\sum_{\boldsymbol{j=1}}^{\boldsymbol{T}} \mathbf{exp}(\boldsymbol{e_{t,j}})} \tag{6}$$

$$\mathrm{c}_t = \sum_{i=1}^{T} \alpha_{t,i} \mathrm{h}_i \tag{7}$$

where the context vector is c_t, the weight vector is v and the hidden state at time step *t* is represented by $\mathrm{e}_{t,i}$, the alignment score is $\alpha_{t,i}$ and the total number of time steps in the input sequence is T. The hyperbolic tangent activation function for the attention mechanism is represented as tanh. Additionally, the weight matrices for the respective gates and the attention mechanism are W_z, W_r, Wh, W_e; the weight matrices for the hidden state and the attention mechanism are U_z, U_r, U_h, U_e; and the bias vectors for the respective gates and the attention mechanism are b_z, b_r, b_h, b_e.

4. PROPOSED RESEARCH METHODOLOGY

The proposed IDS model to detect known, unknown and zero-day attacks in IoMT leverages a GRU with an Attention Mechanism-based DL technique. This comprehensive approach includes data pre-processing, feature extraction using PCA and handling class imbalance with SMOTE. The model is rigorously trained and evaluated, ensuring robustness and reliability through K-Fold cross-validation and hyper-parameter tuning with Keras Tuner, which allows defining an optimized attention function that directly helps priorities the most important features without huge extra computational costs, unlike all other existing attention-based IDS models accessible for IoT and IoMT applications. The following sub-sections provide a detailed breakdown and analysis of the critical components of the operational methodology.

4.1 Proposed IDS-model Architecture

Figure 2 illustrates the proposed IDS model architecture utilizing a GRU with Attention Mechanism-based Hybrid DL technique. This architecture is designed to effectively capture temporal dependencies and highlight significant features in IoMT data. Figures 3 and 4 depict the detailed GRU with Attention Mechanism model layer architecture applied to the ICU Healthcare and NF-TON-IoT datasets, respectively, demonstrating the multiple layers (Input, GRU, Attention and Dense or Output Layers) to construct the robust and secure IDS model for IoMT network.

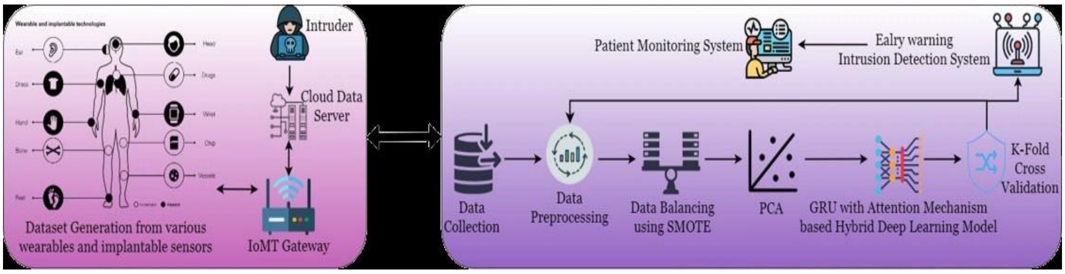
Wearable and implantable technologies
Ear
Dress
Hand
Bone
Feet
Head
Drugs
Wrist
Chip
Vessels
Intruder
Cloud Data Server
Dataset Generation from various wearables and implantable sensors
IoMT Gateway
Patient Monitoring System
Ealry warning Intrusion Detection System
Data Collection
Data Preprocessing
Data Balancing using SMOTE
PCA
GRU with Attention Mechanism based Hybrid Deep Learning Model
K-Fold Cross Validation

Figure 2. Intrusion-detection system's model architecture for IoMT network.

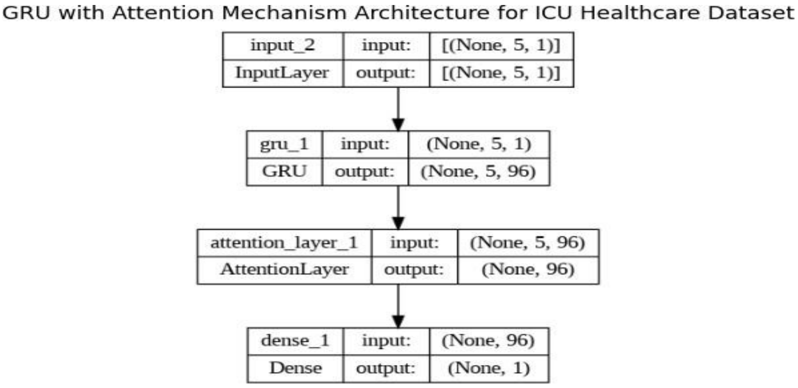
GRU with Attention Mechanism Architecture for ICU Healthcare Dataset
input_2 | input: | [(None, 5, 1)]
InputLayer | output: | [(None, 5, 1)]
gru_1 | input: | (None, 5, 1)
GRU | output: | (None, 5, 96)
attention_layer_1 | input: | (None, 5, 96)
AttentionLayer | output: | (None, 96)
dense_1 | input: | (None, 96)
Dense | output: | (None, 1)

Figure 3. GRU with attention mechanism model layer architecture for ICU healthcare dataset.

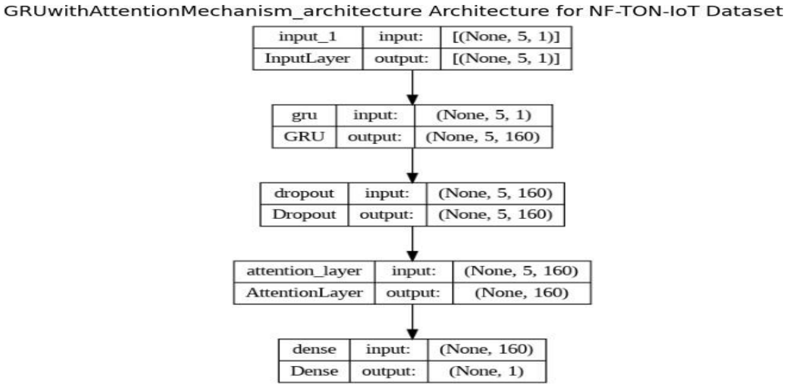
GRUwithAttentionMechanism_architecture Architecture for NF-TON-IoT Dataset
input_1 | input: | [(None, 5, 1)]
InputLayer | output: | [(None, 5, 1)]
gru | input: | (None, 5, 1)
GRU | output: | (None, 5, 160)
dropout | input: | (None, 5, 160)
Dropout | output: | (None, 5, 160)
attention_layer | input: | (None, 5, 160)
AttentionLayer | output: | (None, 160)
dense | input: | (None, 160)
Dense | output: | (None, 1)

Figure 4. GRU with attention mechanism model layer architecture for NF-TON-IoT dataset.

4.2 Proposed IDS Framework

This GRU with an Attention Mechanism-based Hybrid Deep Learning IDS framework presents a comprehensive workflow for addressing known, unknown and zero-day intrusion attacks in real-time IoMT scenarios. It includes data pre-processing, model building and evaluation, feature reduction and performance visualization, providing a detailed approach for enhancing model performance in this critical field. The framework utilizes the ICU Healthcare and NF-TON-IoT datasets to evaluate the effectiveness of the proposed IDS model, ensuring the robustness of the proposed Intrusion Detection Systems in the IoMT network environment. The step-by-step operational phases to construct our proposed secure IDS model for the IoMT network are as follows.

1) **Data Pre-processing**
    a) Cleaning the data by handling infinite, missing and duplicate values and encoding categorical target labels in numerical format.
    b) Balancing the dataset using SMOTE (Synthetic Minority Over-sampling Technique) to address the class-imbalance issue.
    c) Splitting the data into training and testing sets and performing feature scaling.

2) **Feature Extraction Using Principal Component Analysis (PCA)**

    PCA extracts features, lowering the dataset's dimensionality while keeping the essential features for efficient and accurate model training.

3) **Training the GRU with Attention Mechanism-based Hybrid DL Model for Classification**
    a) **Model Architecture:** Constructs and trains the GRU with Attention Mechanism-based hybrid DL model aiming to classify network-traffic data effectively into different categories of network attacks or normal behavior. This model combines:
        i. GRU layers for temporal feature extraction.
        ii. The Attention Mechanism is trained to learn where to pay attention at each time step by aligning the relevant contextual information with the hidden states of GRU.
        iii. Dense layers for final classification.

    b) **Hyper-parameter Tuning**
        i. It utilizes Keras Tuner for hyper-parameter optimization, finding the best configuration for GRU units and dropout rate.
        ii. It uses early stopping, which stops the training process when the model's performance on a validation set reaches an unacceptable level, to prevent overfitting.

    c) **Model Training**
        i. The model is trained on the pre-processed and feature-extracted dataset.
        ii. The model's performance is assessed in depth by utilizing a variety of metrics, including Accuracy, ROC curves, Precision, Recall, F1-Score and Confusion Matrix.

4) **Cross-validation:** The K-Fold cross-validation technique is utilized to rigorously evaluate the model's performance across five different splits of the datasets, ensuring robustness and generalizability.

5) **Handling Noisy Data**
    a) We use Gaussian noise to demonstrate the robustness of the model under noisy conditions with an average of zero and a standard deviation of 0.1 introduced to the features, with the effect of emulating interference related to surroundings and communication networks in IoT systems such as fluctuations in network signals and transmission errors.
    b) A Random Forest Classifier is trained on noisy data to compare performance.
    c) We found the accuracy for instances with the added noise, proving its robustness based on the ICU Healthcare dataset as 99.98% and 99.93% for the NF-TON-IoT dataset.

6) **Performance Visualization**

Algorithm 1 presents a detailed methodology for constructing our advanced Hybrid Deep Learning IDS model incorporating all the above processes tailored specifically for IoMT networks.

Algorithm 1: Algorithm for Intrusion Detection in IoMT

```
Require: Dataset $D$ with features $X \in \mathbf{R}^{m.n}$ and labels $y \in \mathbf{Z}^{m}$ (where $m$ is the number of samples and
    $n$ is the number of features).
Ensure: Trained GRU with Attention Mechanism model
Load and Preprocess Data:
Load dataset D from the CSV file
Separate features X and target y
Select only numeric features. $\mathbf{X}_{\mathbf{numeric}}$
Standardize numerical features using StandardScaler:
    $\mathbf{X}_{\mathbf{scaled}}$ = scaler.fit_transform($X_{\text{numeric}}$)
Dimensionality Reduction with PCA: $\mathbf{X}_{\mathbf{pca}}$ = pca.fit_transform($X_{\text{scaled}}$)
Encode Target Variable using LabelEncoder:
    $\mathbf{y}_{\mathbf{encoded}}$ = label_encoder.fit_transform($y$)
Split Data into Training and Testing Sets: $\mathbf{X}_{\mathbf{train}}$, $\mathbf{X}_{\mathbf{test}}$, $\mathbf{y}_{\mathbf{train}}$, $\mathbf{y}_{\mathbf{test}}$ =
    train_test_split($X_{\text{pca}}$, $y_{\text{encoded}}$, test_size = 0.2, random_state = 42)
Handle Class Imbalance with SMOTE:
    $X_{\mathbf{smote}}$, $y_{\mathbf{smote}}$ = smote.fit_resample($X_{\text{train}}$, $y_{\text{train}}$)
Define and Train GRU with Attention Model:
Define AttentionLayer class
Convert data to NumPy array and reshape for GRU model: $\mathbf{X}_{\mathbf{train\_np}}$, $\mathbf{X}_{\mathbf{test\_np}}$
Define a model-building function for hyperparameter tuning using Keras Tuner to find the
    best model
Train the best model on $\mathbf{X}_{\mathbf{train\_np}}$, $\mathbf{y}_{\mathbf{smote}}$ with EarlyStopping callback
Save and load the trained model
Evaluate the Model on Test Data: $\mathbf{X}_{\mathbf{test\_np}}$, $\mathbf{y}_{\mathbf{test}}$
Calculate and print accuracy, precision, recall, F1-score and AUC-ROC
Visualize loss and accuracy graphs and confusion matrix
Evaluate Model with Noise and Class Imbalance:
Add Random Noise to features and split data into train and test sets
Train and evaluate the accuracy of the Random Forest classifier on noisy data
K-Fold Cross-Validation:
Perform and visualize the K-fold cross-validation scores on five folds to assess model
    generalization
```

5. EXPERIMENTAL SETTING

5.1 Experimental Setup

We utilized a high-performance computing environment to establish a robust experimental setup for our Intrusion Detection System tailored for Internet of Medical Things (IoMT) network communication. This setup featured a 1TB hard drive operating on an Intel Core i7-6700 CPU clocked at 3.40GHz with 8GB RAM, running Ubuntu 20.04.4 LTS for stability and advanced networking capabilities. Leveraging Google Colab, a scalable cloud-based platform renowned for its computational power, facilitated our IDS model's development and simulation phases, accommodating extensive computations and large datasets. We chose Python for its rich ecosystem of libraries supporting machine-learning models, which is crucial for our testing and validation processes. To rigorously assess the effectiveness and accuracy of our IDS model, we conducted experiments using two prominent publicly available benchmark datasets, the ICU Healthcare dataset and the NF-TON-IoT dataset. These datasets are well-regarded for their comprehensive coverage of cyber-attacks across the IoMT network environment, providing critical benchmarks for evaluating our system.

5.2 Dataset Description

5.2.1 ICU Healthcare Dataset

The ICU Healthcare Intrusion Dataset [30] offers a rich source of network-traffic data captured from a simulated ICU healthcare environment, providing valuable insights into cyber-security threats and vulnerabilities in healthcare settings. The dataset consists of the records under three types of network traffic classes: Attack class, Environment-monitoring class and Patient-monitoring class, as depicted in Figure 5. In Figure 6, we have demonstrated the distribution of balanced and unbalanced labeled classes in the ICU Healthcare dataset using SMOTE. The detailed specification of the ICU Healthcare dataset is mentioned below.

1. **Size:** The dataset comprises 1,88,694 network-traffic data records captured over a specific period, providing a comprehensive representation of various network activities within an ICU healthcare environment.
2. **Features:** Each data record includes detailed information about network-traffic attributes in 52 categories such as source IP address, destination IP address, protocol type, timestamp, packet size and network port.
3. **Traffic Composition:** The dataset holds three types of traffic classes: a.) Attack class, b.) Environment-monitoring class and c.) Patient-monitoring class. The Normal class (Environment-monitoring class and Patient-monitoring class) and Attack class of the IoT healthcare dataset hold 1,08,568 and 80,126 records, respectively.
4. **Labels:** The dataset includes labeled instances as 0 (Normal) and 1 (Attack), indicating the presence or absence of cyber-security threats or anomalies in the IoMT-enabled heathcare network traffic. The dataset contains four distinct attack types: Brute Force, MQTT Publish Flood, MQTT Distributed Denial-of-Service (DDoS) and SlowITE [31].

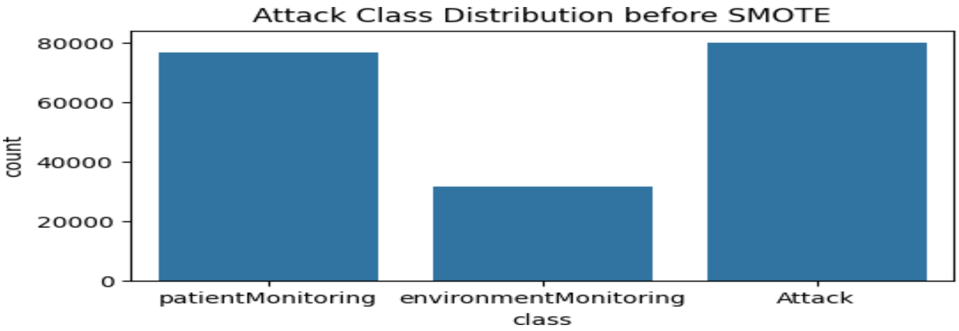

Figure 5. ICU healthcare dataset attack categories.

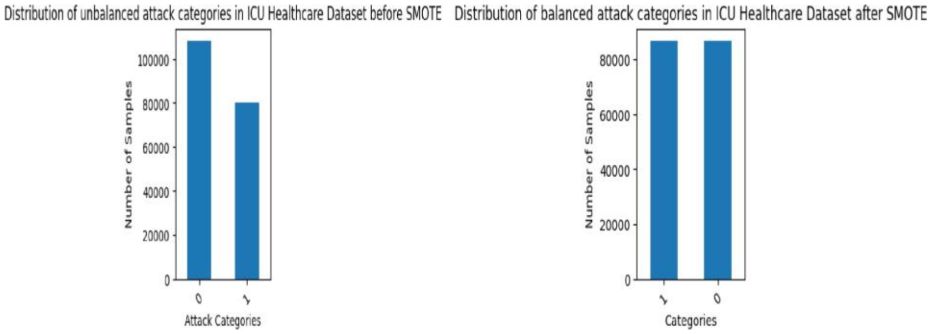

Figure 6. ICU healthcare dataset attack categories, before and after SMOTE.

5.2.2 NF-TON-IoT Dataset

The NF-ToN-IoT dataset offers a comprehensive source of network-traffic data specifically captured from IoT environments. This dataset is essential for understanding cyber-security threats and vulnerabilities within IoT networks. Its availability supports research, development and evaluation of Intrusion Detection Systems (IDSs), Machine-learning models and security measures tailored for safeguarding IoT infrastructure. The dataset comprises records categorized under different types of network-traffic classes, as depicted in Figure 7, providing a valuable resource for anomaly detection and traffic analysis. Figure 8 demonstrates balancing unbalanced distributed labeled classes in the NF-TON-IoT Dataset using SMOTE. A thorough inspection of the NF-TON-IoT dataset is as follows:

1. **Size:** The dataset comprises 1,379,274 network traffic-data records, offering a comprehensive representation of various network activities within IoT environments.
2. **Features:** Each data record includes detailed information about network traffic attributes in 14

categories, such as source IP address, destination IP address, protocol type, packet size, network port, among others.

3. **Traffic Composition:** The dataset includes two types of traffic classes:
   a) **Attack class:** Represents malicious network traffic consisting of DoS, Injection, DDoS, Scanning, Password, MITM, XSS, Backdoor and Ransomware.
   b) **Benign class:** Represents non-malicious, regular network traffic.
4. **Labels:** Labels help in identifying the presence or absence of cyber-security threats or attacks in IoT network traffic:
   a) **0 (Normal):** Indicates benign network traffic.
   b) **1 (Attack):** Indicates malicious network traffic.

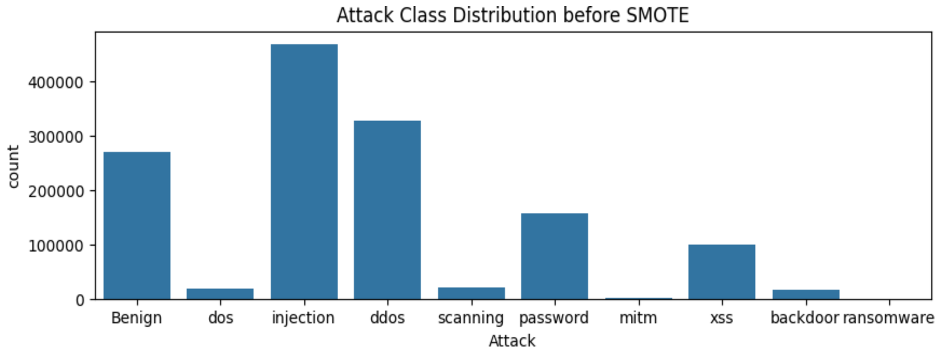

Figure 7. NF-TON-IoT dataset attack categories.

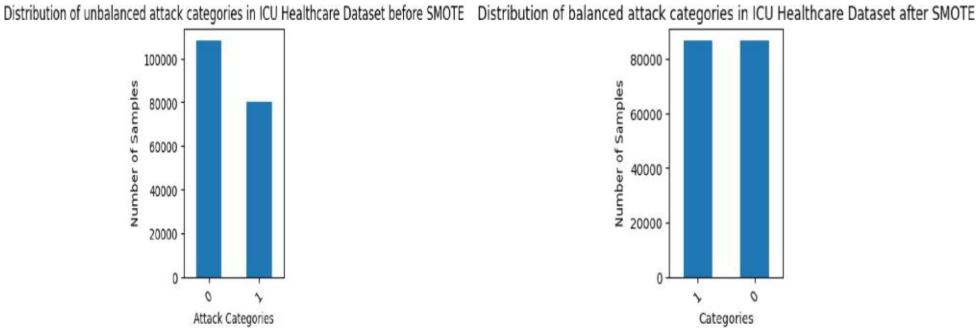

Figure 8. NF-TON-IoT dataset attack categories, before and after SMOTE.

5.3 Performance Evaluation

5.3.1 Performance Metrics

Performance metrics serve as fundamental measures for evaluating the effectiveness of classification models, offering critical insights into the capability of the proposed IDS model to classify instances and detect anomalies accurately. These metrics collectively provide a robust evaluation framework for assessing its real-world efficacy. The key performance metrics include:

1) **Precision (%):** Precision measures how many accurate positive predictions there are among all the positive predictions the model makes. This can be computed as follows:

$$\text{Precision } \% = \left(\frac{TP}{TP+FP}\right) \times 100 \tag{8}$$

2) **Recall (%):** The ratio of true positive predictions to all real positive instances in the dataset is known as recall and it may be calculated as follows:

$$\text{Recall } \% = \left(\frac{TP}{TP+FN}\right) \times 100 \tag{9}$$

3) **F1-score (%):** The F1-score, calculated as follows, is the harmonic mean of precision and recall and offers a fair evaluation of the model's performance.

$$\text{F1} - \text{score } \% = \left(\frac{2TP}{2TP+FP+FN}\right) \times 100 \tag{10}$$

4) **Accuracy (%):** Accuracy reflects the proportion of correctly classified instances among all instances in the dataset, expressed as:

$$\text{Accuracy } \% = \left(\frac{TP+TN}{TP+TN+FP+FN}\right) \times 100 \tag{11}$$

5) **Accuracy with noise (%):** The algorithm for calculating model accuracy when noisy data is included is the same as for conventional accuracy calculation, but it is applied to the predictions produced on the noisy dataset and can be expressed as follows:

$$\text{Accuracy with noise } \% = \left(\frac{TP_{noisy}+TN_{noisy}}{TP_{noisy}+TN_{noisy}+FP_{noisy}+FN_{noisy}}\right) \times 100 \tag{12}$$

6) **Mean K-Fold Cross-validation (CV) Accuracy (%):** The average accuracy ratings from each cross-validation fold are the mean K-Fold cross-validation accuracy. This offers a broader gauge of the model's effectiveness, denoted by:

$$\text{Mean K} - \text{Fold CV Accuracy } \% = \left(\frac{\sum_{i=1}^{K}\left(\frac{TP_i+TN_i}{TP_i+TN_i+FP_i+FN_i}\right)}{K}\right) \times 100 \tag{13}$$

Confusion Matrix

We assess the effectiveness of our suggested classification model using a confusion matrix. By comparing predicted labels with actual labels, it classifies predictions into True Positives (TP), True Negatives (TN), False Positives (FP) and False Negatives (FN). Figures 9 and 10 show the true and predicted values derived from our proposed Hybrid DL IDS model in confusion-matrix format on ICU Healthcare and NF-TON-IoT datasets, respectively.

6. Experiments and Result Analysis

In real-time Internet of Medical Things (IoMT) contexts, the proposed hybrid Deep Learning IDS model based on Attention Mechanism and GRU is designed to identify known, unknown and zero-day attacks. Evaluation of the IDS model utilized the benchmark ICU Healthcare and NF-TON-IoT Datasets. In the operational phase, raw datasets underwent comprehensive pre-processing steps, including data cleaning, normalization and dimensionality reduction using PCA to enhance computational efficiency. Subsequently, the processed data was fed into the GRU with Attention Mechanism for sequence modeling, leveraging its ability to capture intricate temporal dependencies in healthcare-network traffic.

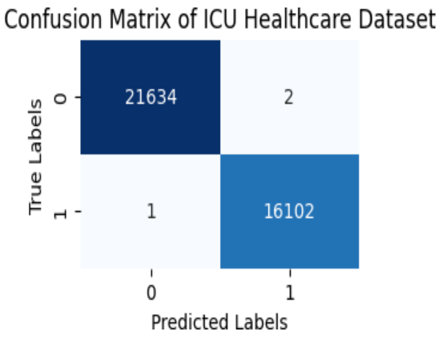

Figure 9. Confusion matrix of ICU healthcare dataset.

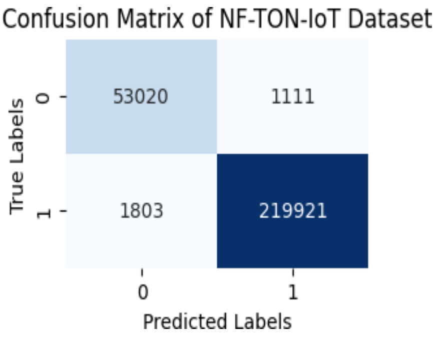

Figure 10. Confusion matrix of NF-TON-IoT dataset.

Table 3. Classification report of the proposed IDS model on both the given datasets.

Dataset	Precision (%)	Recall (%)	F1-score (%)	Accuracy (%)	Accuracy with Noise (%)	Mean K-Fold CV Accuracy (%)	Support
ICU Healthcare Dataset	99.98	99.99	99.99	99.99	99.98	99.99	37739
NF-TON-IoT Dataset	99.50	99.17	99.34	98.94	99.93	97.30	275855

The evaluation of the proposed IDS model demonstrates robust performance across multiple metrics and datasets. The accuracy achieved by the ICU Healthcare and NF-TON-IoT datasets reached 99.99% and 98.94%, respectively. Precision, Recall, F1-score, Accuracy with Noise and Mean K-fold cross-validation accuracy results are summarized in the Classification Report as shown in Table 3. The GRU with Attention Mechanism-based Hybrid DL IDS model was trained for 20 epochs on both datasets, maintaining consistent loss and accuracy trends throughout each epoch. Figures 11 and 12 illustrate dataset loss and accuracy graphs, showcasing the model's learning process and convergence over time.

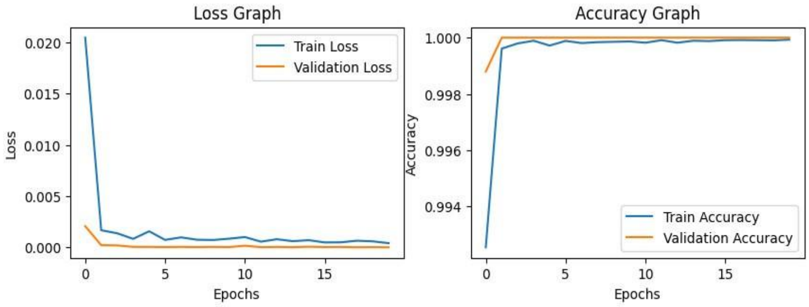

Figure 11. Loss accuracy graph for ICU healthcare dataset.

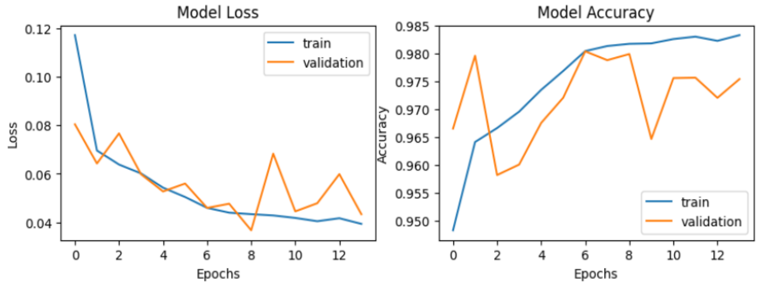

Figure 12. Loss accuracy graph for NF-TON-IoT dataset.

Table 4. Results comparison of state-of-the-art IDS techniques with proposed IDS model on IoMT devices.

References	**Dataset**	**Technique**	**Precision (%)**	**Recall (%)**	**F1-score (%)**	**Accuracy (%)**	**Accuracy with Noise (%)**	**CV Accuracy (%)**
Kumar *et al.* [14]	TON-IoT	Ensemble Learning	90.54	99.98	95.03	96.35	. . .	. . .
Khan *et al.* [18]	TON-IoT	Ensemble Learning	. . .	. . .	. . .	98.56	. . .	. . .
Awotunde *Et al.* [22]	NF-TON-IoT	Swarm-Neural-Network	. . .	. . .	. . .	89.00	. . .	. . .
Proposed	NF-TON-IoT	Hybrid Deep Learning	99.50	99.17	99.34	**98.94**	99.93	97.30
Khan *et al.* [21]	ICU Healthcare	Hybrid Deep Learning	96.34	99.11	100.00	99.83	. . .	. . .
Saran *et al.* [23]	ICU Healthcare	Deep Learning	…	…	…	99.00	…	…
Proposed	ICU Healthcare	Hybrid Deep Learning	99.98	99.99	99.99	**99.99**	99.98	99.99

Five splits for K-fold cross-validation were employed to assess the robustness and generalizability of the proposed IDS model. They obtained a Per-fold accuracy score and a mean K-fold accuracy score of 99.99% for the ICU Healthcare dataset and 97.30% for the NF-TON-IoT datasets, respectively, as depicted in Table 3. This analysis ensures the model performs consistently well across different data splits, reinforcing its reliability in diverse IoMT environments. Table 4 compares the proposed IDS model with the existing techniques for various attack-detection capabilities and performance metrics on ICU Healthcare and NF-TON-IoT datasets.

In summary, the experimental results validate the effectiveness and reliability of the proposed GRU with Attention Mechanism-based Hybrid DL IDS model for detecting intrusions in IoMT networks. The model’s ability to handle complex healthcare data, robust performance metrics and comparative analysis against existing techniques underscores its potential as a critical security measure in modern healthcare infrastructures.

7. Conclusion and Future Scope

Securing Internet of Medical Things (IoMT) networks against known, unknown, and zero-day intrusion attacks is crucial for maintaining patient-data privacy and operational integrity in healthcare environments. In response to these challenges, we have developed and evaluated a sophisticated IDS model for IoMT applications, integrating PCA for dimensionality reduction, SMOTE for handling imbalanced datasets and a GRU with Attention Mechanism for sequence modeling. As shown in Table 3, at Section 6, our suggested IDS model performs admirably across a variety of evaluation criteria, including Precision. This research work produced a suitable model for testing new datasets by incorporating changes in the model to Recall, F1-score, Accuracy, Accuracy with noise and K-Fold Cross-validation Accuracy. We showed the model’s effectiveness in detecting various types of intrusions while lowering false positives and false negatives, with 99.99% accuracy for the ICU Healthcare dataset and 98.94% accuracy for the NF-TON-IoT dataset. The evaluation of the IDS model also incorporated the analysis of Accuracy with noise and K-Fold Cross-validation Accuracy. By introducing noise into the dataset, we assessed the robustness of the model, ensuring that it maintains high accuracy even under adverse conditions, as 99.98% for the ICU Healthcare dataset and 99.93% for the NF-TON-IoT dataset. The K-Fold Cross-validation provided a comprehensive evaluation by training and validating the model across multiple data splits, resulting in an average accuracy of 99.99% for the ICU Healthcare dataset and 97.30% for the NF-TON-IoT dataset, demonstrating the model’s consistent performance. We can accommodate several amendments for further enhancement and exploration to include new attack approaches to achieve robust applicability in real-life IoT and IoMT scenarios. We can test a light version of the proposed IDS model with fewer GRU units and attention layers to decrease the demands on the resources used while retaining the high detection rate of real-time intrusion detection, especially in resource-constrained IoMT environments.

Acknowledgements

Thanks are due to Dr. Nishtha Kesswani, for her invaluable guidance, unwavering support and insightful feedback throughout this research. Her expertise and encouragement have been instrumental in completing this work.

References

[1] F. Laricchia, "Topic: Wearables," Statista, [Online], Available: https://www.statista.com/topics/1556/wearable-tec, Accessed: Jun. 18, 2024.

[2] R. Dwivedi, D. Mehrotra and S. Chandra, "Potential of Internet of Medical Things (IoMT) Applications in Building a Smart Healthcare System: A Systematic Review," Journal of Oral Biology and Craniofacial Research, vol. 12, no. 2, pp. 302-318, 2022.

[3] S. S. Ambarkar and N. Shekokar, "Toward Smart and Secure IoT Based Healthcare System," Proc. of Internet of Things, Smart Computing and Technology: A Roadmap Ahead, Studies in Systems, Decision and Control, vol. 266, pp. 283-303, Springer, 2020.

[4] A. Tabassum, A. Erbad, A. Mohamed and M. Guizani, "Privacy-preserving Distributed IDS Using Incremental Learning for IoT Health Systems," IEEE Access, vol. 9, pp. 14271-14283, 2021.

[5] R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum and J. Qadir, "Security and Privacy of Internet of Medical Things: A Contemporary Review in the Age of Surveillance, Botnets and Adversarial ML," Journal of Network and Computer Applications, vol. 201, p. 103332, 2022.

[6] M. L. Hernandez-Jaimes et al., "Artificial Intelligence for IoMT Security: A Review of Intrusion Detection Systems, Attacks, Datasets and Cloud-Fog-Edge Architectures," Internet of Things, vol. 23, p. 100887, 2023.

[7] M. Wazid, A. K. Das, J. J. Rodrigues, S. Shetty and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," IEEE Access, vol. 7, pp. 182459-182476, 2019.

[8] A. Si-Ahmed et al., "Survey of Machine Learning Based Intrusion Detection Methods for Internet of Medical Things," Applied Soft Computing, vol. 140, p. 110227, 2023.

[9] Y. Rbah et al., "Machine Learning and Deep Learning Methods for Intrusion Detection Systems in IoMT: A Survey," Proc. of the 2022 2nd IEEE Int. Conf. on Innovative Research in Applied Science, Engineering and Technology (IRASET), pp. 1-9, Meknes, Morocco, 2022.

[10] K. Gupta et al., "A Tree Classifier Based Network Intrusion Detection Model for Internet of Medical Things," Computers and Electrical Engineering, vol. 102, p. 108158, 2022.

[11] J. Nayak, S. K. Meher, A. Souri, B. Naik and S. Vimal, "Extreme Learning Machine and Bayesian Optimization-driven Intelligent Framework for IoMT Cyber-attack Detection," The Journal of Supercomputing, vol. 78, no. 13, pp. 14866-14891, 2022.

[12] S. Liaqat et al., "SDN Orchestration to Combat Evolving Cyber Threats in Internet of Medical Things (IoMT)," Computer Communications, vol. 160, pp. 697-705, 2020.

[13] I. A. Khan et al., "XSRU-IoMT: Explainable Simple Recurrent Units for Threat Detection in Internet of Medical Things networks," Future Generation Computer Systems, vol. 127, pp. 181-193, 2022.

[14] P. Kumar et al., "An Ensemble Learning and Fog-cloud Architecture-driven Cyber-attack Detection Framework for IoMT Networks," Computer Communications, vol. 166, pp. 110- 124, 2021.

[15] S. Nandy et al., "An Intrusion Detection Mechanism for Secured IoMT Framework Based on Swarm-neural Network," IEEE J. of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1969-1976, 2021.

[16] P. Singh et al., "Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT," IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 722-731, 2022.

[17] S. A. Wagan et al., "A Fuzzy-based Duo-secure Multi-modal Framework for IoMT Anomaly Detection," J. of King Saud Uni.-Computer and Information Sciences, vol. 35, no. 1, pp. 131-144, 2023.

[18] F. Khan et al., "A Secure Ensemble Learning-based Fog-cloud Approach for Cyberattack Detection in IoMT," IEEE Transactions on Industrial Informatics, vol. 19, no. 10, pp. 10125 – 10132, 2023.

[19] U. Zukaib et al., "Meta-IDS: Meta-learning Based Smart Intrusion Detection System for Internet of Medical Things (IoMT) Network," IEEE Internet of Things J., vol. 11, no. 13, pp. 23080 – 23095, 2024.

[20] S. P. RM et al., "An Effective Feature Engineering for DNN Using Hybrid PCA-GWO for Intrusion Detection in IoMT Architecture," Computer Communications, vol. 160, pp. 139-149, 2020.

[21] S. Khan and A. Akhunzada, "A hybrid DL-driven Intelligent SDN-enabled Malware Detection Framework for Internet of Medical Things (IoMT)," Computer Comm., vol. 170, pp. 209-216, 2021.

[22] J. B. Awotunde et al., "A Deep Learning-based Intrusion Detection Technique for a Secured IoMT System," Proc. of the Int. Conf. on Informatics and Intelligent Applications (ICIIA 2021), Part of the Book Series: Communications in Computer and Information Science, vol. 1547, pp. 50-62, Nov. 2021.

[23] N. Saran, N. Kesswani and R. Saharan, "Intrusion Detection System Using Deep Learning Techniques for Internet of Medical Things (IoMT)," Proc. of the International Conference on Deep Learning, Artificial Intelligence and Robotics (ICDLAIR 2023), Part of the Book Series: Lecture Notes in Networks and Systems, vol. 1001, pp. 752-763, Springer, Aug. 2024.

[24] Y. K. Saheed and M. O. Arowolo, "Efficient Cyber Attack Detection on the Internet of Medical Things-smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms," IEEE Access, vol. 9, pp. 161546-161554, 2021.

[25] R. Chaganti et al., "A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things," Sustainability, vol. 14, no. 19, p. 12828, 2022.

[26] J. A. Alzubi, O. A. Alzubi, I. Qiqieh and A. Singh, "A Blended Deep Learning Intrusion Detection Framework for Consumable Edge-centric IoMT Industry," IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 2049 – 2057, 2024.

[27] F. Laghrissi, S. Douzi, K. Douzi and B. Hssina, "IDS-attention: An Efficient Algorithm for Intrusion Detection Systems Using Attention Mechanism," Journal of Big Data, vol. 8, no. 1, p. 149, 2021.

[28] M. V. Assis et al., "A GRU Deep Learning System against Attacks in Software Defined Networks," Journal of Network and Computer Applications, vol. 177, p. 102942, 2021.

[29] X. Miao, S. Li, Y. Zhu and Z. An, "A Novel Real-time Fault Diagnosis Method for Planetary Gearbox Using Transferable Hidden Layer," IEEE Sensors Journal, vol. 20, no. 15, pp. 8403-8412, 2020.

[30] F. Hussain et al., "IoT Healthcare Security Dataset," IEEE Dataport, [Online], Available: https://ieee-dataport.org/keywords/healthcare-security-dataset, 2021.

[31] F. Hussain et al., "A Framework for Malicious Traffic Detection in IoT Healthcare Environment," Sensors, vol. 21, no. 9, p. 3025, 2021.

ملخص البحث:

لقد أدّى انتشار أجهزة إنترنت الأشياء في الرّعاية الصّحّية، وبخاصّة إنترنت الأشياء الطّبّية، إلى إحداث ثورةٍ في أنظمة رعاية المرضى والمراقبة الصّحّية. إلّا أنّ تكامل هذه الأجهزة الطّبّية المتّصلة بعضها ببعض قاد إلى إدّخال تحدّياتٍ غير مسبوقة تتعلّق بأمن البيانات، الأمر الذي يؤكّد الحاجة إلى أنظمةٍ متينةٍ لاكتشاف التّسلُّل لحماية بيانات المرضى والبنية التحتية للرعاية الصّحّية. ولحماية أجهزة إنترنت الأشياء الطّبّية من العديد من الهجمات، قام الباحثون بتطوير أنظمةٍ عديدةٍ لاكتشاف التّسلُّل لاختراق تلك الأجهزة والحصول على بيانات حسّاسة على نحوٍ غير مشروع. ومع ذلك، فإنّ تطوير نظامٍ فعّالٍ ومتينٍ لاكتشاف التّسلُّل يظلّ تحدّياً بحدّ ذاته.

نقترح في هذه الورقة نظاماً لاكتشاف التّسلُّل لإنترنت الأشياء الطّبّية باستخدام وحدة التّكرار المبوّبة مع تقنية التّعلُّم العميق الهجينة القائمة على آلية الانتباه. وقد أجريت تجارب عملية على النّظام الهجين المقترح، وبرهن على أداءٍ ممتازٍ في حماية بيانات أجهزة إنترنت الأشياء الطّبّية من الهجمات السّبرانية المختلفة. وجرى تقييم النّظام المقترح على بعض مجموعات البيانات في مجال الرّعاية الصّحّية، وذلك باستخدام عددٍ من مؤشرات الأداء، بما فيها الدّقّة، إلى جانب مقارنة النّظام المقترح بعددً من الأنظمة المشابهة الواردة في دراسات سابقة أخرى، حيث أثبت النّظام المقترح تفوّقاً ملحوظاً على غيره من الأنظمة بتحقيقه مؤشّرات أداءٍ عالية، مما يؤكّد متانته وفعاليته، وبالتّالي نجاعته في حماية أجهزة إنترنت الأشياء الطّبّية من الهجمات والاختراقات.