INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Hybrid Intelligent Anomaly Detection System Using Attention based Deep Learning Approach for Cyber Attacks Prevention

N Girubagari[1]*, T N Ravi[2], S Panneer Arokiaraj[3]

1 Research Scholar, Department of Computer Science, Thanthai Periyar Government Arts and Science College, Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India
2 Associate Professor, Department of Computer Science, Jamal Mohamed College, Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India
3 Associate Professor, Department of Computer Science, Thanthai Periyar Government Arts and Science College, Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India

OPEN ACCESS

Received: 09-07-2024

Accepted: 20-09-2024

Published: 08-10-2024

Citation: Girubagari N, Ravi TN, Arokiaraj SP (2024) Hybrid Intelligent Anomaly Detection System Using Attention based Deep Learning Approach for Cyber Attacks Prevention. Indian Journal of Science and Technology 17(38): 3947-3959. https://doi.org/10.17485/IJST/v17i38.2224

* **Corresponding author**.

ngiruba@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: Network Intrusion Detection System (NIDS) plays an important role in finding and preventing cyber-attacks, which helps to improve the entire security posture of an organization's network infrastructure. The development of Deep Learning (DL) techniques possess the ability of IDS to detect attacks without delay and protects from intrusions even in real-time environment. **Methods:** The present study proposes an improved IDS framework called Enhanced Gated Recurrent Unit Hyper-Model combined Attention Bidirectional Long-Short Term Memory (EGHAB) approach, to effectively address the detection of attacks with maximum accuracy and minimal error rate. The proposed model is enhanced by using methods like numericalization and normalisation for pre-processing the input data, Genetic Algorithm (GA) for extracting intricate features from the input data, and the EGHAB classifier, which works on the principles of both Gated Recurrent Unit (GRU) and Bidirectional Long-Short Term Memory (BiLSTM) models along with attention mechanism. **Findings:** The EGHAB model efficiently learns the abnormal behaviour of network and classified the attack and non-attack data using the publicly available NSL-KDD dataset and a generated real time data set, scapy. And it achieved 99.94% accuracy over NSL KDD dataset during multiclass classification and 93.3% on real time data set with reduced Error rate. Additionally, to examine the efficacy, the proposed approach is compared with other existing methods and proved its improved performance. **Novelty:** A combined ensemble classifier with GRU, BiLSTM and attention mechanism is designed to predict the attacks in earlier stage rather than due over. The model achieved better accuracy and reduced false assumption using anomaly prediction mechanism.

Keywords: Cyber Attack; Anomaly Detection; Deep learning; Gated Recurrent Unit; Bi Directional Long-Short Term Memory; Attention mechanism

1 Introduction

In modern era, the advanced IoT paradigm has gained an extensive adoption in smart cities. Whereas, the smart city's network traffic through IoT systems is increasing drastically, producing new cyber security problems, as these IoT devices are being associated with sensors, which are directly associated with enormous cloud servers. Hence, cyber-attacks are becoming more sophisticated, targeting systems that process or store sensitive information. With the exponential increase in cyber-attacks, the design of a detection mechanism can detect the harmful effect and attacks[1]. Whereas, the combination of IT (Information Technology) with OT (Operational Technology) in crucial infrastructures enhances sustainability, consumer-centricity and efficiency at the expense of enhanced cyber-attack susceptibility.

Thus, to handle these vulnerable intrusions, it is highly essential to develop an IDS with improved accuracy and reduced False Alarm Rate (FAR). Anomaly-based detection approaches are the most valuable technology to prevent the target system and networks from harmful activities. Anomaly prediction is concerned with finding data patterns that significantly diverge from the expected behaviour. Identifying Denial of Service (DoS) and Probe attacks are the major critical security challenges experienced by network technologies. When compared with Machine Learning (ML), DL algorithms play a significant part in detecting the intrusions in earlier stage, by learning the attack behaviours by extracting the network features using opt mechanism. Additionally, by extracting the hidden network behaviour, the FAR is also gradually decreased[2,3].

The study[4] proposed a NIDS using LSTM model with 1-n encoding and Extract Transform Load (ETL) for preprocessing. It has been tested and trained on the benchmark data set NSL KDD and achieved 99.98% accuracy. But its training time became very high. And in study[5], LSTM has been considered as an effective approach in detecting the intrusions by using Mutual Information (MI), Principal Component Analysis (PCA). However, to achieve high accuracy in less training time, only two features have been considered by the proposed model. An adaptive DL model with a combination of Convolutional Neural Network (CNN), LSTM, Recurrent Neural Network (RNN) and Gated Recurrent Unit (GRU)[6] has been proposed later. It learned only the high-level features from the given time sequential data. Even though it gives better results, it takes more time to convert the unbalanced data into a balanced one and gives importance only for binary classification.

The study[7] has employed the BiLSTM based DL algorithm with data pre-processing steps, in order to choose the characteristics to use and train the model. In addition, the multi head attention mechanism has also been utilized to train the model with essential input features. One more study[8] has introduced an intrusion detection technique according to RNN, namely, CNN, BiLSTM and attention mechanism. These networks have been applied to extract both the spatial and temporal features and to enhance the accuracy of the classifier. The study has also suggested that model classifier has been trained by using loss function to pay special attention to even minority class data. However, the model could not predict the new unlabelled attacks.

Contrastingly, a novel Deep Supplement GRU (DSGRU) based model has been proposed[9] for IoT intrusions. The proposed model has used the original GRU and a decoded GRU and the effective softmax activation function that has played an important role for the extraction of effective features from the IoT network traffic data. The model achieved better performance on attacks detection. But the model is experimented only on IoT network and did not consider the early forecasting of attacks. Similarly, a network intrusion detection model based on CNN, GRU and double layer Feature extraction based Fusion selection (FF) has been proposed in[10]. It used an altered focal loss function to handle the unbalanced data. However, the feature fusion process which is to be refined in order to increase the operating efficiency of the model.

The existing study[11] has introduced a TGA hybrid model using the Temporal Convolutional Network(TCN), BiDirectional GRU (BiGRU) and self-attention mechanisms as an unsupervised approach in order to detect the anomaly from the network traffic sequences. The proposed model has used TCN for the local temporal information and the BiGRU for global temporal information. Hence, the detection algorithm can find the anomalies that span across numerous time scales. While the accuracy of prediction of attacks was attractive, the proposed model has less effective classification on small samples. Similarly, the study[12] has introduced an efficient deep learning anomaly prediction mechanism by Attention -Emotion-Embedding BiLSTM-GRU combination. Though, the combination has been used in sentiment analysis, the study provided an idea for novelty to incorporate the same for intrusion detection systems.

1.1. Research Gaps

To sum the discussion, although several approaches, either LSTM, BiLSTM or GRU along with or without attention mechanism were involved in detecting attacks in network systems, these methods lack in detecting large number of attacks with lower training samples.

Even though the previous research works achieved better accuracy either for binary classification or for multiclass classification or for both categories, all models required high convergence time even for balanced data set and could not predict the attacks in advance.

It is also observed that methods that involved DL approaches struggle in achieving highly improved accuracy rate and low FAR in detecting attacks that are collected from real-systems.

1.2. Major Contributions

To overcome the issues gathered through the literature review, the main motive of the present study is to develop an **E**nhanced **G**ated Recurrent Unit **H**yper-Model Combined **A**ttention **B**idirectional Long-Short Term Memory (EGHAB) model with the following strategies to perform attack detection effectively:

- Pre-processing the input data by using numericalization and normalisation to convert the input categorical values into numerical values for efficient classification of attack and normal classes.
- Feature selection using GA approach, to select the most significant and relevant features from the pre-processed data.
- Classification based on hybrid method of GRU hyper model and Attention based BiLSTM for improved multiclass classification of attacks and its detection.
- Evaluate the efficacy of proposed EGHAB model, by computing relevant metrics namely accuracy, precision, recall, F1-score & FAR using NSL-KDD dataset and a Real-time dataset.

2 Methodology

Generally, the network security is complex for traditional anomaly based detection approaches to find the unknown threats due to inaccurate feature extraction of network traffic. The IDS is considered as the most significant tool in handling large scale and complex network attacks, but lack of detection based on real time data set hinders its further development. Moreover, the previous phase of the proposed approach has been dealt with a NIDS using parallel Altered BiLSTM(ABILSTM) and Combined Bidirectional GRU(CBIGRU)[13] with limited performance efficiency. Thus, an improved anomaly detection approach using deep learning concept is introduced here to prevent cyber attacks efficiently . The enhanced GRU Hyper-Model combined Attention BiLSTM approach is designed specifically to detect the malicious attacks by monitoring the abnormal behaviour of the network with improved detection accuracy and low FAR in both publicly available dataset and real-time dataset. Implementing GA into the training process of DL model helps in optimizing the model's parameters more efficiently. This hybrid approach leverages the strengths of both GA and DL to produce a more robust and effective anomaly detection system for cyber-attack prevention. The overall process and methods involved in proposed approach is exemplified in Figure 1.

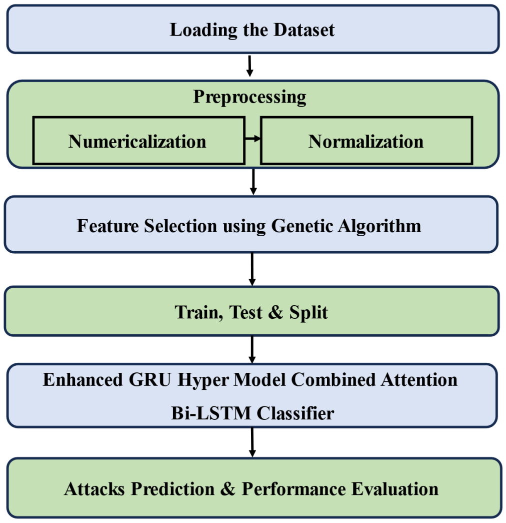

Loading the Dataset
Preprocessing
Numericalization
Normalization
Feature Selection using Genetic Algorithm
Train, Test & Split
Enhanced GRU Hyper Model Combined Attention Bi-LSTM Classifier
Attacks Prediction & Performance Evaluation

Fig 1. Illustration of Overall Process Involved in Proposed Approach

2.1. Dataset Description

2.1.1. NSL – KDD Dataset

The enhanced and newer version of KDD99, the NSL-KDD dataset is represented as the new benchmark dataset[14] that comprises of KDD Train+ including 125,973 records along with KDD Test+ including 22,544 records. Moreover, each record is signified by almost 41 features belonging to four different feature groups. These groups include basic features, Content features, time based and connection based traffic features. In cybersecurity community, each record is represented as the connection between the two pairs among two hosts present in the network. Appropriately 21 predicted label class for each record denotes the normal and attack record. The training dataset comprises of 24 different types of attacks, while the test dataset includes additional 14 types of attacks that are not included in train data. This is done to test the ability of the classifier to recognise the unknown attacks intruding into the network. KDDTest-21 dataset is the subset of KDD Test+ and is more complex for classification process. Table 1 shows the record description of NSL-KDD dataset.

Table 1. Description of NSL-KDD Dataset

Record Details	KDD Train+	KDD Test+	KDD Test-21
Total	125,973	22,544	11,850
Normal	67343	9711	2152
DoS	45927	7458	4342
Probe	11656	2421	2402
R2L	995	2754	2754
U2L	52	200	200

2.1.2. Real-Time Dataset Using Scapy Package

The Python Scapy is a potent packet modification tool and a powerful library used for effectively manipulating the packets, which is built on Python software. It allows to create, transfer, capture and analyse the network packets traffic at different levels of network stack. It is also significant as Scapy can be used to perform malicious activities, where packet manipulations can be done[15]. So, the proposed work uses the traffic generator Scapy to generate the packets and spoof the source IP address of the packets by using k-means clustering technique. Initially, the selection of 'k' based on the cluster requirements is done, where $k-means > 1$. The set of k-means is determined as $n_1, \ldots ..n_{k-means}$, where each observation is combined to specific point. The new mean of the centroids of observations present in the new clusters are computed by using Equation (1) and then the average of each observation generates the least sum of squares within the cluster which is given by Equation (2). Further, the cluster centre is updated as shown in Equation (3).

$$\mu_i = \frac{1}{|n_i|}\sum\nolimits_{x \epsilon n_i} x \tag{1}$$

$$E = \sum\nolimits_{i=1}^{k-means} \frac{1}{2}\sum\nolimits_{x\, \in n_i} || \, x - \mu_i||^2 \tag{2}$$

$$center_a = \frac{\sum y_i}{p} \tag{3}$$

where

- x : Data point
- k : Number of clusters.
- n_i : Data points belonging to the index cluster.
- μ : Centroid of the index cluster.
- $\|x - \mu_i\|^2$: Squared Euclidean distance between data point and centroid.
- E : error or distortion
- $Center_a$: improved cluster center

- Σy_i : Quantity of centroidss.
- y_i or all clusters.
- p :Total number of clusters.

The new centroids are compared with centroids, which have been computed earlier and their difference is obtained and the process is repeated until convergence condition occur. The algorithm ends and the output of k-means cluster centre values are obtained. Thus, by clustering the output data produced by k-means clustering approach, the real-time dataset is developed. It allows for the creation of diverse and realistic network traffic patterns. It consists of approximately 100,000 packets, captured over a period of 1 hour, with a size of around 10 GB. It includes normal traffic patterns and different types of attacks, confirming an inclusive depiction of distinctive network conditions. It has a set of columns with a certain value. Some of the columns of scapy are Source Address (src), Destination Address (dst), Flags, Version, Internet Header Length (IHL), Fragmentation (Frag), and Protocol. In terms of diversity, the dataset includes a wide range of protocols (TCP, UDP, ICMP, etc.), packet sizes, and network behaviors (e.g., HTTP, FTP, SSH, etc.). Through pretending actual data flows, the dataset permits for a precise evaluation of the ability of proposed EGHAB model to identify the anomalies in the legitimate traffic. This diversity ensures that the model is exposed to various real-world network conditions, making it more robust and generalizable. The count of both normal and attacks collected through real-time dataset, Scapy, is represented by the additional heatmap, which shows the correlation among each data as illustrated in Figure 2.

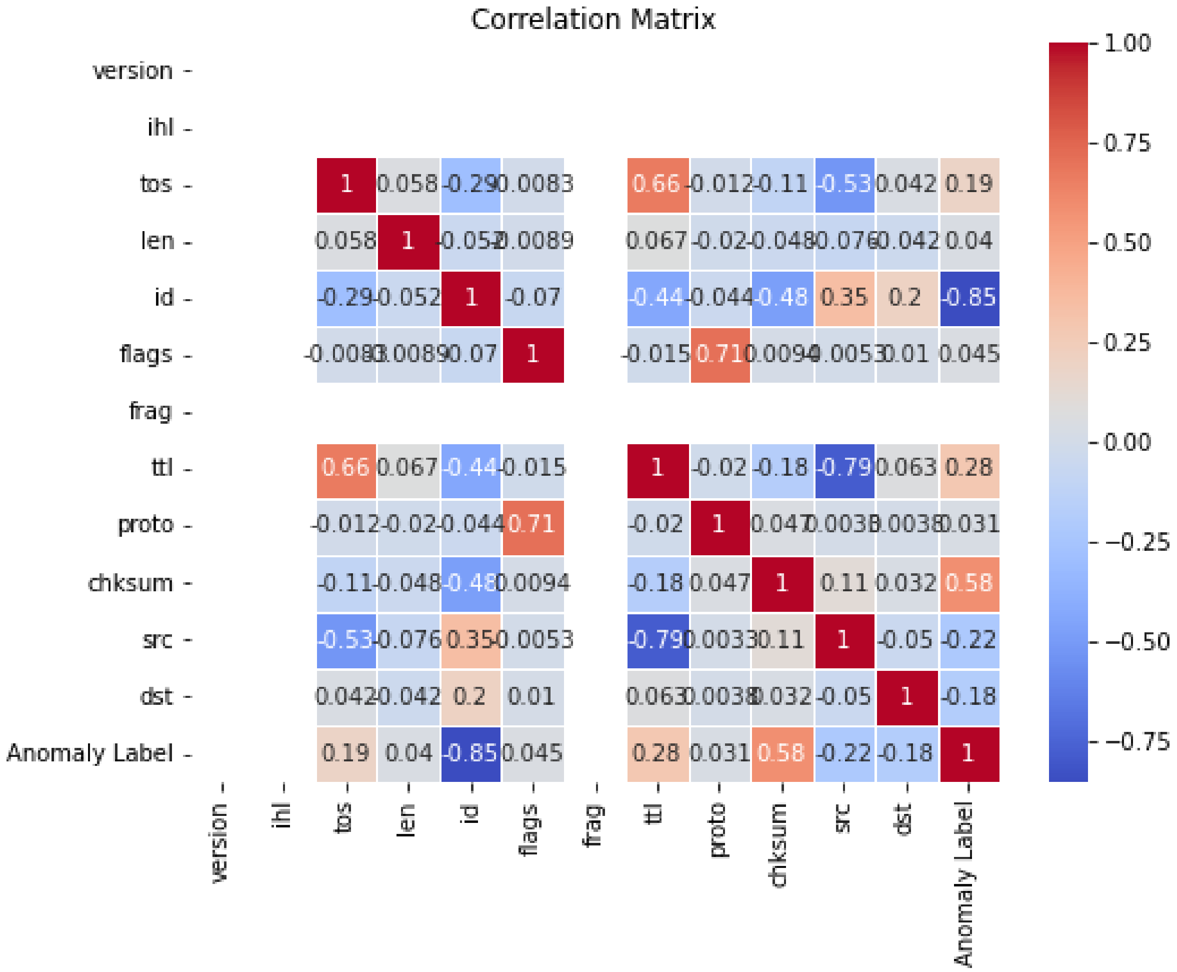


Fig 2. Heatmap of Real-Time Dataset 'Scapy'

2.2. Data Pre-processing

Usually, the intrusion detection systems become complicated while processing entire data retrieved from the input raw data of each dataset. This is due to the presence of large volume of network traffic. It may also consists of either categorical or numerical values. So, the proposed method involves a data preprocessing stage to expedite training of input data to generate optimal solution and performance. This stage consists of two steps which are data numericalization and normalization.

- **Numericalization**[15] **:** The data numericalization process is applied to convert the categorical values into numerical values, making simpler data for the model to process. In addition, numericalization process is done with label encoder, in which unique numeric values are assigned to categorical values by label encoding. In some cases, the numericalized data attributes comprises of small feature values and some consist of large values. The variation among minimum and maximum feature value is very huge and this difference influences the original feature values.
- **Normalization**[15] **:** The normalisation process is included in preprocessing stage to avoid the effectiveness of original feature values on attacks detection. So, the characteristics of numerical data are scaled to a specific range in the process of data normalisation like [0-1], [-1,1]. This is done to ensure that the features are on the scale and thus helps in decreasing the training time.

2.3. Genetic Algorithm Based Feature Selection

In this approach, the feature selection is performed using GA on the prescribed datasets to effectively select the most significant features for precise classification process. The GA is comprised of following steps:

- The **initial population** comprises of feature chromosomes where the chromosomes are generated randomly. The number of initial populations is restricted, as many categories of attacks are included.
- Further, **fitness function** f$_j$ is computed, which provides an outlook to predict the features with low similarity among all the features as in Equation (4).

$$f_j = \frac{a_j + (1 - m_j)}{2} \tag{4}$$

Besides, the a_j signifies the precision of jthfeature, m_j, a measure of the correlation between the jth feature and other features in the dataset. While $(1-m_j)$indicates the un-correlation or lack of correlation between the jth feature and other features, $a_j+(1-m_j)$combines the precision and the complement of correlation for the jth feature. It computes the average of these two values, possibly to balance the importance of precision and un-correlation in evaluating the fitness of the jth chromosome. By taking the average, it ensures that both precision and un-correlation contribute to the final score.

- The **selection process of parents** is directly proportional to fitness function values, which denotes that if fitness value is high (1), the chances of selection is also high.
- Further, 50 % **mutation** and 50% **crossover rate** are involved in the next generation of population.
- Three GA operators, selection, crossover, and mutation are continued until the stopping condition 'fittest population' is attained.

2.4. Enhanced GRU Hyper-model Combined Attention BiLSTM (EGHAB classifier)

Generally, using GRU architecture can save computing resources and training time as well as the Bidirectional LSTM architecture to effectively improve the classification accuracy. By involving GRU, an effective and comprehensive feature learning can be performed and thus can produce an enhanced outcome in detecting the intrusion of malicious attacks. The layers of BiLSTM, would eliminate the unwanted duplicate information with the help of the output features from both the past and future time steps and make the classification of attacks effective[13]. Thus, the proposed EGHAB model utilises the incorporation of GRU approach with BiLSTM module along with attention mechanism. This is done since large number of dimensions are present in the feature space and this tends to drastically impact the learning performance of the classifier, especially in the real-time environment. Simultaneously, this enables the proposed EGHAB model to make interpretation of input data easier, reduce computational complexity and train faster.

The reset gate of GRU controls how much of the previous hidden state information should be discarded or reset before considering the current input. The hidden state, on the other hand, is the output of the GRU cell and represents the current state of the model given by the amalgam of the input at the current time step and the previous hidden state[16]. The hidden state (a long-short term memory) is hyper-modelled to learn the independent representation of individual series depending on the specific information. The study implements the matrix representation of GRU instead of vector at each step. This matrix representation has involved increased parameters and it makes the Hyper GRU more effective. The Hyper GRU is represented as a set of parallel GRU, in which each module processing one individual series focuses on sequence classification. Therefore, Hyper GRU algorithm of dimensionality reduction is applied here on the original input dataset to decrease the input features. The output from the hyper GRU model comprises of some redundant information which are irrelevant to detection task.

On the other hand, the BiLSTM comprises of various small constructions with one basic LSTM unit including four layers, input, forward propagation, backward propagation and the output layers. The output features from both the past and future time steps makes the classification of attacks effective[17]. In addition of bidirectional layers, the newly added attention layer focuses the most relevant parts of the input sequence and ignore the unwanted sequences. Further, to avoid the repetitive information produced by hyper GRU module, the output of Hyper GRU is passed into Attention based BiLSTM module. With the help of the altered gate functions, the proposed model detects attacks by monitoring the abnormal behaviour of the networks and devices connected to it. The attention based BiLSTM along with Hyper GRU model as shown in Figure 3 works well by comprehensively extracting the features from the input data and learning those features in a sequential manner.

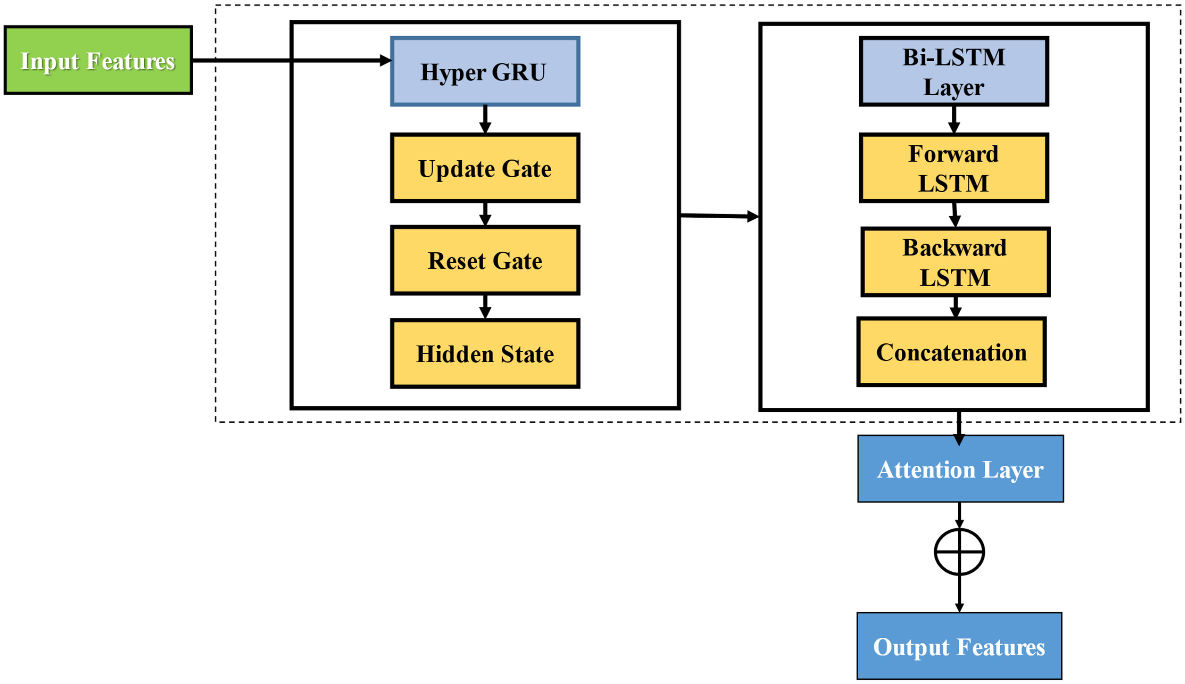


Fig 3. Hyper GRU Model Combined Attention BiLSTM Architecture

To represent the Hyper GRU, the hidden state is given as matrix with time step t, $H_t = \left[h_t^1, \ldots .h_t^{N+1}\right] T$, in which $H_t \in R^{(N+1)\times d}$. The $h_t^n \in R^d$ represents the hidden state vector mapping, where d is signified as hidden dimension of all input features $n = 1, 2 \ldots .N+1$. Thus, the hidden state of GRU cell is computed as, $D = (N+1) \times d$. For Hyper GRU network, the previous hidden state matrix and newly emerging input data, the cell update H_t^- are shown as in Equation (5).

$$R_t = \sigma(m_r \otimes H_{t-1} + V_r \otimes x_t + b_r)$$

$$k_t = \sigma(m_z \otimes H_{t-1} + V_z \otimes x_t + b_z)$$

$$H_t^- = tanh(m_h \otimes (R_t \odot H_{t-1} + V_h \otimes x_t + b_h))$$

$$H_t = (1 - k_t) \odot H_{t-1} + k_t \odot H_t \tag{5}$$

Where, k_t is the update gate, R_t is the reset gate and H_t deliberates hidden state matrix and H_t^- is the memory state. Similar to the hidden state matrix, all gates possess same shape. Here, $m* \in R^{(N+1)\times d\times d}$ is represented as the hidden-to-hidden transition tensor, and input-to-hidden transition tensor is given by $V* \in R^{(N+1)\times d\times 1}$, while $m*\otimes H_{t-1} and V*x_t$ are the information that are captured from preceding hidden state and from newly emerging data.

The generated hidden states are then transferred to attention based BiLSTM layer, in which the attention function focusses on retrieving the significant features and increasing the ability of the classifier by learning in a sequential order.

The feature matrices ω^v and ω^t are multiplied to acquire modal information matrix, A_1, A_2, where “.” denotes the matrix multiplication.

$$A_1 = \omega^v \cdot (\omega^t)^T, \quad A_2 = \omega^t \cdot (\omega^v)^T \tag{6}$$

Through the softmax activation function, the attention distributions are computed, $M_1, M_2 \in R^{u\times u}$, where $M_1(i,j)$ and $M_2(j,i)$ representing the relationship among the different features and the interaction between them and the significant fusion information, where i denotes the word embedding modality feature and j denotes the visual modality feature.

$$M_1 = softmax(A_1), M_2 = softmax(A_2) \tag{7}$$

Further, the feature matrix multiplies attention distribution to produce the final attention representation matrices, O_1 and O_2.

$$O_1, O_2 \in R^{u\times d_m}, \; O_1 = M_1 \cdot \omega^t, \quad O_2 = M_2 \cdot \omega^v \tag{8}$$

Then multiplication gate method is applied to acquire mutual attention information matrix $C_1, C_2 \in R^{u\times d_m}$ with element wise matrix multiplication $\odot$ and given by Equations (6), (7), (8) and (9).

$$C_1 = O_1 \odot \omega^v, C_2 = O_2 \odot \omega^t \tag{9}$$

By transferring and combining $C1$ and $C2$ to the preferred dimensions, the fused information representation are obtained as shown in Equation (10).

$$Cma_{tv} = (C_1)T \oplus (C_2)T \tag{10}$$

Where, $\oplus$ denotes the combination process of vectors. And the obtained representation matrix includes the weights among the two varying classes depending on feature's prior knowledge on the BiLSTM. It also focusses on modelling and capturing the data's temporal dependencies. Finally, the dense layer receives the input from previous layers and is used to classify the classes based on the output from the proposed preceding layers. Thus, the collected samples are then passed into softmax activation function for interpreting the probability distribution of the samples. During the training process, regularization methods are applied between layers to directly prevent overfitting by modifying the model's weights. L1 (Lasso) and L2 (Ridge) regularization techniques include a consequence to the loss function based on the magnitude of the model coefficients. Specifically, L1 regularization led to spare the proposed model by forcing some weights to zero, while L2 regularization prevents weights from becoming extremely large, thereby controlling model complexity. Additionally, early stopping with a patience of 5 epochs is implemented to prevent overfitting and halt training when the model's performance on the validation set starts to degrade. The Enhanced Deep Learning Algorithm of the proposed model can be summarized as follows:

Step 1: Define input layer with specified shape.
Step 2: Reshape input data to match the expected shape.
Step 3: Define a custom HyperGRU layer.
Initialize HyperGRU with parameters units, dropout, and recurrent_dropout.
Utilize a GRU layer with specified dropout rates.
Return the Hidden states' information.
Step 4: Apply multiple Bidirectional LSTM layers using Modelmergeattentionlayer function.
Input: x (tensor), num_layers, units, return_sequences, dropout, recurrent_dropout Loop from 1 to num_layers:
Add Bidirectional LSTM layers to x with specified parameters.
Return the modified tensor after applying all LSTM layers.

Step 5: Add a custom AttentionLayer to compute attention weights.
Initialize AttentionLayer with parameters units.
Initialize dense layers W, U, and V within AttentionLayer
Step 6: Add additional dense layers for further processing
Step 7: Calculate context vector using attention mechanism.
Step 8: Define Output layer with softmax activation for multi-class classification.
Step 9: Compile the model with Adam optimizer with learning rate 0.001 and sparse categorical crossentropy loss.
Step 10: Train the compiled Model using training data (x_train, y_train) by specifying the number of epochs =10, batch size = 64, and validation data.

3 Results and Discussion

The results produced by the computation of proposed EGHAB Model is deliberated in this section. The NSL KDD dataset and a scapy based real time data set are used for the evaluation of the proposed model.The execution of the process is done in Spyder 3.7 environment. In the proposed algorithm, an Adam optimizer is used, which stands for "Adaptive Moment Estimation". Due to the use of Adam optimizer, the optimization algorithm is iterated in order to reduce the loss function during neural network training. To project the effectiveness of the present method, comparison of existing approaches with proposed model are also exposed.

The performance metrics such as Accuracy, Precision, Recall, F1- score and FAR[13] are considered here for the evaluation of the efficiency of the proposed EGHAB approach. After the suitable selection of datasets and performance metrics for the evaluation of the proposed model, the most significant features that are selected through proposed feature selection process are then passed into train and test phases. In this stage, the input data are divided into two splits called train and test split in the ratio of 80:20, where 80% of data are used for training the classifier and 20% for testing the actual value and the predicted value. In addition, KDD TEST 21 data set is used as the validation data set to avoid the overfitting problem. This ensures that both the datasets are representative of entire dataset and provides the effective measure of accuracy prediction of the trained classifier and unseen testing set. While the model is being used for validation on the test set, it is trained on the training set. Fit with training on a model. The selected features by the Genetic Algorithm (GA) on NSL-KDD dataset and for real time data set generated by Scapy package are shown in Table 2.

Table 2. Features Selection using GA on NSL-KDD & Real Time Dataset ' Scapy'

Dataset	Total Number of Features	No. of Features Selected by GA	Selected Features
NSL – KDD	41	14	[1 3 4 5 6 11 23 26 27 29 30 31 34 37]
Scapy	50	5	[0 1 2 4 6]

The results procured by the proposed enhanced GRU Hypermodel Combined Attention BiLSTM model can be classified into two categories: (i) Binary classification which consists of Normal and Attacks classes and (ii) Multiclass Classification which consists of normal and four classes of attacks.

3.1. Binary Classification

For the binary classification, the train set records are classified into only two classes, normal and attacks. Similarly, the test set also. Only the features selected during the preprocessing stage by the GA, as listed in Table 2, are used in the evaluation phase. The confusion matrix for proposed model on NSL-KDD dataset and on Real time data set are represented in Figure 4. It is a type of matrix that compares the actual target values with the predicted values produced by the proposed approach, which shows that the actual and predicted values are almost similar to each other as shown in Figure 4. Misclassification of attack and normal classes are not found, revealing enhanced classification of proposed approach with NSL-KDD dataset.

Further, the obtained results of the proposed model on NSL KDD data set in terms of performance metrics are measured as 99.93, 99.92, 99.96, 99.05 and 0.016 percentage of accuracy, precision, recall, F1-score and FAR respectively. Likewise, the achieved results in terms of accuracy is 93.3, precision of 92.2, recall of 93.6, F1-score of 92.5 and FAR value is 0.045 on real time data set. It is regarded from the result that, the detection of attacks and non-attacks in the dataset are effectively performed by the proposed EGHAB. The obtained percentages also concluded that, the proposed model can predict and classify attacks and normal data with minimum classification error rate even on real time data set.

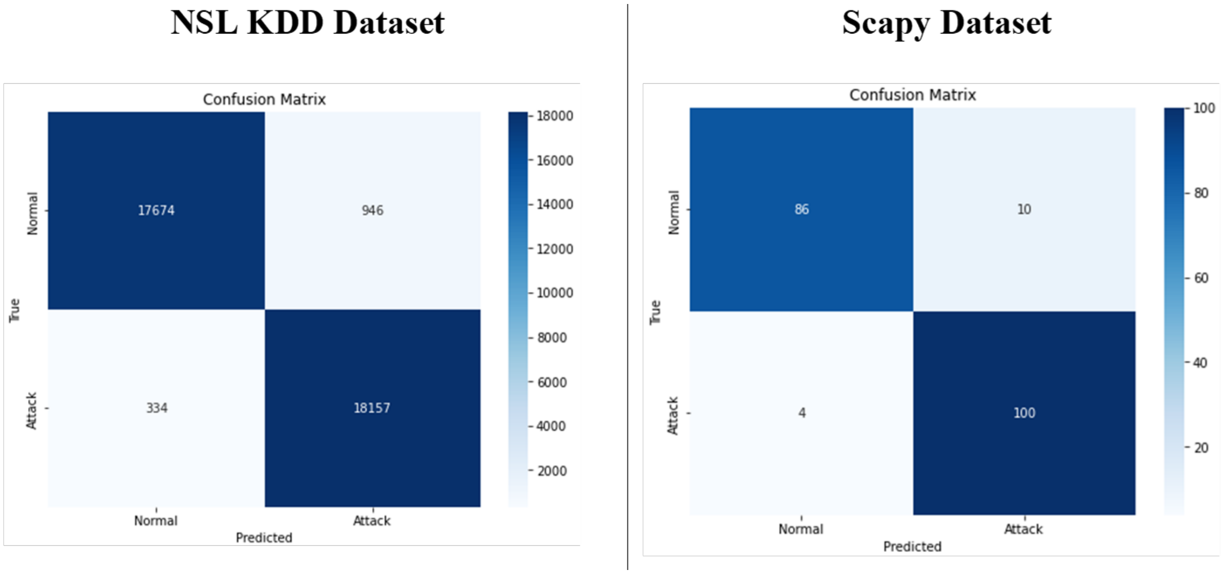
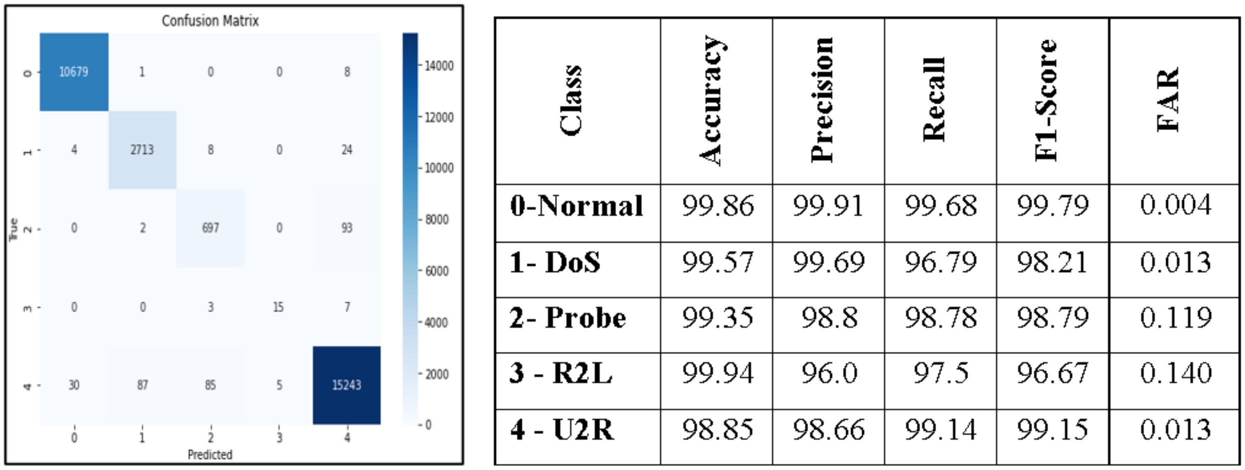


Fig 4. Confusion Matrix of EGHAB on NSL KDD Dataset and Scapy Dataset

3.2. Multiclass Classification

During normalization, the preprocessing stage of the proposed model, the features are categorized into five classes with predicted labels. The numerals 0, 1, 2, 3, and 4 are used as labels for representing the classes - Normal, DoS, Probe, R2L and U2R attacks respectively. The performance of the multi-class classification data set can be summarized using a confusion matrix, which compares the predicted labels with the actual labels that is shown in Figure 5. In the multi-class confusion matrix, the rows represent predicted labels and the columns represent actual labels of attack classes. Each cell in the matrix indicates the number of instances falling into a specific predicted-actual label combination. Moreover, multi-class confusion matrices can be used to calculate other performance metrics like accuracy, precision, recall, F1-score and FAR for each class.

The evaluation results of proposed model on NSL KDD data set are also tabulated in Figure 5. It represents the internal results of the performance of the proposed model for each class. Accuracy rate for normal and anomaly classes have higher values, as well as higher precision value. Classes 0 and 3 have higher precision values, and class 0 have higher recall and F1-score values. The proposed model achieves low FAR for all the classes.



Class	Accuracy	Precision	Recall	F1-Score	FAR
0-Normal	99.86	99.91	99.68	99.79	0.004
1- DoS	99.57	99.69	96.79	98.21	0.013
2- Probe	99.35	98.8	98.78	98.79	0.119
3 - R2L	99.94	96.0	97.5	96.67	0.140
4 - U2R	98.85	98.66	99.14	99.15	0.013

Fig 5. Confusion Matrix and Internal Results of EGHAB for Multi-class Classification on NSL KDD data set

3.3. Comparative Analysis

In order to access the performance of the proposed EGHAB approach, it is compared with existing algorithms and the results procured are shown in Table 3 and is projected in the form of graphical representation in Figure 6. The existing approach implemented IDS using XGBoost[15] algorithm with Preprocessing using numericalization and normalization approach achieved the classification accuracy upto 90% with NSL KDD dataset. While the proposed approach applied on the same dataset obtained average accuracy of 99.94% showing effect analysis of intrusions from input data.

Further, a comparison of proposed EGHAB model with conventional LSTM[5], BILSTM[7] and BILSTM[8] along with attention mechanisms shows that, the existing approaches attained a maximum accuracy of 85.65%, 94.7%, 99.79% respectively, whereas the EGHAB model achieved 99.94 % accuracy. Even though the accuracy level looks same in both the models, earlier model has a high False Alarm Rate 0.034%, while the proposed model has a reduced False Alarm Rate 0.015%. Likewise, the comparative analysis of the earlier models using GRU and BiLSTM with Attention Mechanisms[11,12] shows that, from 93% to 97.83% accuracy has been achieved and the operating efficacy and computational complexity became their issues and the model evaluation did not give importance for the FAR computations. However, the proposed model considered the computational complexities like overfitting, training time during model construction phase and tried to overcome the issues using training, testing and validation sets of input data and of Feature selection concept using standard Genetic algorithm with a ratio of 50-50 of crossover and mutation rate.

Additionally, Table 3 shows that, the PACENIDS model based on parallel Altered BiLSTM and Combined Bidirectional GRU approaches, which was developed as the previous phase of the proposed model had achieved the maximum accuracy of 96.59, whereas the proposed EGHAB model achieves an increase in that accuracy and decrease in FAR, that exhibits the improved performance of the proposed model. The proposed model used mechanisms for both the preprocessing and feature selections, while the previous approach followed a feature selection algorithm but did not give importance for the preprocessing of input data.

Table 3. Comparison of Proposed EGHAB Model with Existing models

Model	Accuracy	Precision	Recall	F1-Score	FAR
XGBoost[15]	89.63	97.73	87.23	93.21	0.022
LSTM[5]	85.65	86.00	86.00	85.00	-
CNN + LSTM[6]	82.60	94.90	68.90	79.80	-
BiLSTM[7]	95.13	96.00	97.00	97.00	-
BiLSTM+ Attention[7]	94.70	95.00	98.00	96.00	-
CNN + BiLSTM+ Attention[8]	99.79	-	99.83	-	0.340
GRU[9]	77.42	80.61	77.42	75.03	-
BiGRU+ Attention[11]	97.83	97.85	97.83	97.57	-
GRU+ BiLSTM[12]	93.00	91.00	94.00	92.00	-
PACENIDS[13]	96.59	94.69	96.67	96.93	0.027
Proposed EGHAB	99.94	99.69	96.61	98.21	0.015

As per the above results, the proposed system has the values of 0.99, 0.99, 0.96, 0.98 and 0.015 for accuracy, recall, F1-score, precision and FAR respectively. The performance metrics of the proposed EGHAB system remains better and the accuracy level of the proposed system is 99.94%, which is higher than the existing models.

The proposed EGHAB model is introduced for an efficient detection of intrusion in complicated settings. To optimize and scale for larger datasets, proposed EGHAB employs an integrated design by including the extra units and layers to accommodate the increasing data complexity. It employs batch processing to manage large dataset effectively and integrates data amplification approaches to improve different data training. The regularization techniques will aid avoid overfitting, while the rates of adaptive learning enhance convergence speed.

Furthermore, the Transform Learning (TL) permits the proposed EGHAB model to minimizing the training time and strengthen pre-trained models. By incorporating these features, EGHAB can efficiently handle larger datasets and more complex network environments, making it suitable for real-world intrusion detection applications.

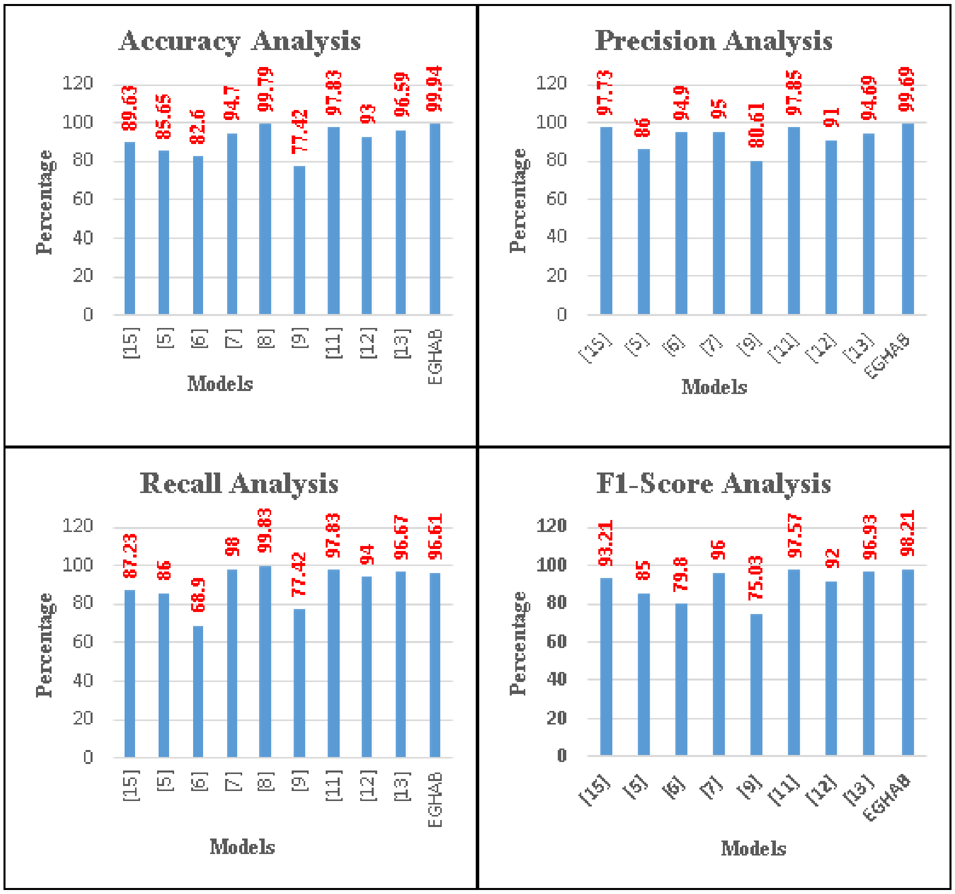


Fig 6. Comparative Analysis of proposed EGHAB Model

4 Conclusion

An enhanced EGHAB model has been developed to effectively address the issues of detecting the intrusions in the network systems. The proposed model integrates the working principles of both GRU and BiLSTM models, paired with Attention based mechanism, enabling it to capture the long-term dependencies of the features from the input datasets and to eliminate redundant unwanted details and thus produced faster and accurate classifier. The notable selected features used as inputs aided the proposed EGHAB model classifier to attain its improved efficiency and accurate detection rate. The suggested model's novel approach combines deep learning techniques on NIDS with enhanced analysis of both normal and attacked data, allowing for early attack prediction using anomaly detection mechanisms. The experimental results consistently demonstrated that the EGHAB model outperforms other conventional attack classification algorithms with the aid of benchmark NSL-KDD dataset.

The proposed approach achieves an accuracy of 99.94 with precision of 99.69, recall of 96.61 and F1-score of 98.21 and FAR of 0.015. It results in 3 to 4% increase in accuracy and up to 1 to 2% decrease in FAR than the state -of- arts methods. The proposed EGHAB model is able to classify the normal and anomalies with improved accuracy even with real-time data. The same is experimented and the model achieved 93.3% accuracy on real time data set generated using scapy package. In Today's rapidly changing world, there are many chances of unwanted nuisances from the hackers which are to be avoided within a quick fraction of point of time before they affect the entire system. In future research work, the operating efficiency of the cyber attacks classifier 'Hyper GRU-BILSTM-Attention' could be enhanced by implementing various deep learning algorithms with a combination of different preprocessing techniques to achieve 100% accuracy as well as a decline in training and testing time.

References

1) Fredj OB, Mihoub A, Krichen M, Cheikhrouhou O, Derhab A. CyberSecurity attack prediction: a deep learning approach. In: and others, editor. 13th international conference on security of information and networks. 2020;p. 1–6. Available from: https://doi.org/10.1145/3433174.3433614.
2) Xu H, Sun L, Fan G, Li W, Kuang G. A Hierarchical Intrusion Detection Model Combining Multiple Deep Learning Models With Attention Mechanism. *IEEE Access*. 2023. Available from: https://doi.org/10.1109/ACCESS.2023.3290613.
3) Bouyeddou B, Harrou F, Kadri B, Sun Y. Detecting network cyber-attacks using an integrated statistical approach. *Clustering Computing*. 2021;24:1435–53. Available from: https://doi.org/10.1007/s10586-020-03203-1.
4) Boukhalfa A, Abdellaoui A, Hmina N, Chaoui H. LSTM deep learning method for network intrusion detection system. *International Journal of Electrical and Computer Engineering*. 2020;2020(3):3315–3322. Available from: http://doi.org/10.11591/ijece.v10i3.pp3315-3322.
5) Laghrissi F, Douzi S, Douzi K, Hssina B. Intrusion detection systems using long short-term memory (LSTM). *Journal of Big Data*. 2021;8(1):65–65. Available from: https://doi.org/10.1186/s40537-021-00448-4.
6) Meliboev A, Alikhanov J, Kim W. Performance evaluation of deep learning based network intrusion detection system across multiple balanced and imbalanced datasets. *Electronics*. 2022;2022(4):515–515. Available from: https://doi.org/10.3390/electronics11040515.
7) Zhang J, Zhang X, Liu Z, Fu F, Jiao Y, Xu F. A Network Intrusion Detection Model Based on BiLSTM with Multi-Head Attention Mechanism. *Electronics*. 2019;12:4170–4170. Available from: https://doi.org/10.3390/electronics12194170.
8) Dai W, Li X, Ji W, He S. Network Intrusion Detection Method Based on CNN-BiLSTM-Attention Model. *IEEE Access*. 2024;12:53099 –53111. Available from: http://dx.doi.org/10.1109/ACCESS.2024.3384528.
9) Liu Y, Lan Y, Yang C, Ding Y, Li C. A New DSGRU-Based Intrusion Detection Method for the Internet of Things. *Electronics*. 2023;12(23):4745–4745. Available from: https://doi.org/10.3390/electronics12234745.
10) Imrana Y, Xiang Y, Ali L, Noor A, Sarpong K, Abdullah MA. CNN-GRU-FF: a double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units. *Complex & Intelligent Systems*. 2024;2024:1–18. Available from: https://doi.org/10.1007/s40747-023-01313-y.
11) Song Y, Luktarhan N, Shi Z, Wu H. TGA: a novel network intrusion detection method based on TCN, BiGRU and attention mechanism. *Electronics*. 2023;12(13):2849–2849. Available from: https://doi.org/10.3390/electronics12132849.
12) Kabra B, Nagar C. Attention-Emotion-Embedding BiLSTM-GRU network based sentiment analysis. *Journal of Integrated Science and Technology*. 2023;11(4):1–7. Available from: https://pubs.thesciencein.org/journal/index.php/jist/article/view/a563.
13) Girubagari N, Ravi TN. Parallel ABILSTM and CBIGRU Ensemble Network Intrusion Detection System. *International Journal of Intelligent Engineering & Systems*. 2024;17(1):93–93. Available from: https://doi.org/10.22266/ijies2024.0229.10.
14) Khan MM, Alkhathami M. Anomaly detection in IoT-based healthcare: machine learning for enhanced security. *Scientific Reports*. 2024;14(1):5872–5872. Available from: https://doi.org/10.1038/s41598-024-56126-x.
15) Fuhnwi GS, Revelle M, Izurieta C. Improving Network Intrusion Detection Performance: An Empirical Evaluation Using Extreme Gradient Boosting (XGBoost) with Recursive Feature Elimination. In: and others, editor. IEEE 3rd International Conference on AI in Cybersecurity (ICAIC). IEEE. 2024;p. 1–8. Available from: https://doi.org/10.1109/ICAIC60265.2024.10433805.
16) Myint O, Kamolphiwong M, Kamolphiwong S, Vasupongayya T, S. Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN). *Journal of Computer Networks and Communications*. 2019;2019(1):8012568–8012568. Available from: https://doi.org/10.1155/2019/8012568.
17) Liu Y, Dai Y. Deep Learning in Cybersecurity: A Hybrid BERT–LSTM Network for SQL Injection Attack Detection. *IET Information Security*. 2024;2024:1–16. Available from: https://doi.org/10.1049/2024/5565950.