Educational Administration: Theory and Practice
2024, 30(4), 8705-715
ISSN:2148-2403
https://kuey.net/

Research Article

Rooting Out Intruders Using Deep Learning Through RNN And Bilstm

S. Pariselvam[1*], R. Sathishkumar[2], K. Abitha[3], E. V. Akshana[4], S. Thisha[5]

[1*,2,3,4,5]Department of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India, *Email: pariselvam@gmail.com, Email: sathishmail26@gmail.com, Email: suprajakumaresan@gmail.com, Email: akshana2002@gmail.com, Email: thisha1710@gmail.com

Citation: S. Pariselvam, et al. (2024), Rooting Out Intruders Using Deep Learning Through RNN And Bilstm, *Educational Administration: Theory and Practice*, *3*(4), 8705-715
Doi: 10.53555/kuey.v30i4.2808

ARTICLE INFO

ABSTRACT

Protecting networks from harmful activity and illegal access is critical in the field of cybersecurity. As the first line of defense in this regard, intrusion detection systems (IDS) are essential. Distinguishing between benign and malevolent activity, however, is one of the major problems IDS faces, particularly in light of the growing complexity of cyberthreats. Although deep learning techniques show great potential, they are frequently plagued by overfitting, a phenomenon in which a model fits well on training data but does not generalize to new data. A unique framework that combines conventional machine learning methods with RNN and LSTM algorithms has been created to address this difficulty. When it comes to identifying temporal dependencies in network traffic, RNN and LSTM are especially useful. This is essential for identifying risks that are changing. The framework may identify malicious behaviour more accurately by fusing various neural network topologies with conventional machine learning techniques. Another important component of the framework is feature engineering, which is the process of identifying and modifying pertinent features from unprocessed data. This procedure enhances the IDS's overall accuracy by lowering false positives. A number of public datasets, including ISCX-IDS 2012, CICIDS2017, and CICIDS2018, have been used to thoroughly analyse the framework, showing its performance and efficiency. The model delivers outstanding performance measures, such as an accuracy of 96.3%, Precision of 96.83%, and F1-score of 97.5%, through intensive training and validation. Its 98.1% recall rate demonstrates how well it works to reduce false negatives, which is important for early detection. It ensures network security and integrity by providing a more potent protection against the dynamic array of cyberthreats.

Keywords—Recurrent Neural Networks, Deep Learning, Intrusion Detection System, cyberattacks, hybrid algorithm.

1. INTRODUCTION

Numerous tools and methods, such as different IDS, have been created for cloud security in order to counteract vulnerable assaults. The investigation of several intrusion detection systems, which are capable of alerting network managers to both known and unknown threats, is the main emphasis of this research. Intrusion detection systems can be categorized as network-based, host-based, hypervisorbased, or distributed. While host-based systems only detect traffic on a single host, network-based monitoring keeps an eye on all network traffic. [2]. IDS uses methods for detection that are hybrid, anomaly, and signature based. While anomaly-based strategies concentrate on the current user's actions to identify disruptions, signature-based techniques detect intrusion by comparing established patterns or a predefined set of rules [3]. DL algorithms perform at a higher level than ML algorithms [11, 12], examined, the significance of several DL methods was determined, and each algorithm's performance in the intrusion detection area was analyzed. The primary disadvantage of false-positive and zero-day attacks can also be resolved by employing an effective DL algorithm. This study provides a brief overview of various AI-based network and cloud intrusion detection techniques. It compares ML, DL, and ensemble learning-based IDS and evaluates and categorizes various AI-based IDS.A taxonomical

overview of all AI-based intrusion detection systems is also provided. The improvement of prediction performance, reduction of computing time, and improved data understanding are the main reasons for the development of diverse data mining approaches and effective NIDS. In order to attain the desired outcomes, fewer input variables are used, which lowers the cost of computational modeling and improves performance. The NSL KDD dataset contains a substantial amount of data that need modification. There are two primary methods for selecting features: supervised and unsupervised. The goal variable is ignored by the unsupervised feature selection method, which instead focuses on the correlation between the input variables [18, 19]. Using the target variable, supervised feature selection eliminates their pertinent characteristics. Shallow learning demonstrated his incapacity to address environmental issues in real time because to the massive volume of data entries. Because of this, the number of deep learning models, including RNNs, Variation auto encoders, and LSTMs, has grown in recent years. In order to address the shortcomings of the simple machine learning approach and provide effective intelligent abnormality detection (ID) system to counter emerging threats in networks, this paper proposes an algorithm that functions as an ID system using LSTM RNN and encoded in Python.

Using the NSL-KDD dataset the most recent version of the KDD'99 dataset the accuracy, detection rate, and false alarm rates of the generated ID model are also assessed. Labels 1 and 0 denote typical and deviant behaviors, respectively. A confusion matrix is used to display the categorization results. The RNN-LSTM approach has been shown to be the most secure and accurate (96.3%) when compared to other approaches. Furthermore, the parameters of our model are easily changeable; initially, the values are given, but subsequently, the algorithm modifies the values. As a result, the execution time is quite brief. The features that were removed from the dataset during training can be accurately learned by the LSTM model.. This feature allowed the model to distinguish between network assaults and routine traffic with accuracy. The algorithm relies on a multilayer learning sequence that illustrates the RNN's ability to describe the relationship between recent and historical occurrences and identify anomalies and uncommon attack types.

2. RELATED WORK

The increasing complexity and sophistication of cyber threats in today's interconnected digital ecosystem is the reason behind intrusion detection systems, or IDS. Promising findings have been obtained from several experiments in this field, such as convolutional neural networks with decision tree algorithm, multi-task learning, and models based on anomalies. Moreover, Long Short Term Memory and Recurrent Neural Networks can be used to accurately classify intrusion detection. Many DL models are used to identify and classify threats [19]. (CNNs), attention-based frequency models, and multitask learning are frequently used in studies to get good outcomes. Moreover, models based on deep residual networks have a lot of potential to increase anomaly accuracy.

Using the G-ABC with the DNN, Nishika Gulia et al. (2023) [1] demonstrated an enhanced IDS for the cloud. The creation of the G-ABC with DNN is part of the suggested approach to identify the various attacks. The best characteristics from the dataset have been chosen using the G-ABC algorithm. Using the min-max technique, the proposed model is split into multiple phases to label and normalize the input NSL-KDD and UNSW-NB15 datasets. By comparing various criteria, including accuracy, precision, recall, and F-measure, to seven attack statistics taken from two datasets, the suggested IDS's performance has been assessed. It is noted that the average accuracy for various attacks stayed at 98.23%, while the precision, recall, and F-measure were at 99%, 99%, and 99%, respectively.

With the exception of random forests and decision trees, Sabbir Hossain et al. (2023) [2] shows that the neural network model outperforms other common machine learning models in terms of accuracy. The model has the potential to improve intrusion detection accuracy as well as the capacity to determine the type of intrusion. Because there are no duplicate data points in the NSL KDD dataset, we can determine that the model's maximum accuracy is 97.23%. We obtained the highest accuracy (89.2%) from the Random Forest (RF) approach and the lowest accuracy (73.5%) from the KNN algorithm. Currently, the DT approach has the highest Fl score (92%), while the Naive Bayes (NB) algorithm has the lowest score (72%), according to the Fl score analysis of machine learning algorithms.

In 2023 Mary Anita E.A. [3] listed the methods used to ensure security are classified, as are the current AI-based intrusion detection systems. Artificial intelligence (AI)based security measures outperformed conventional security mechanisms in terms of detection and categorization. It looks at how crucial feature reduction is to intrusion detection effectiveness. Since all AI-based processes require feature reduction as a necessary step to get correct results, ML, DL, and ensemble-based AI-based techniques demonstrated very identical above 99% results. It only included the most prevalent and common security attacks, like DoS, Probe, R2L, and U2R. Only the accuracy measurements are used to compare the AI-based systems.

The 2022 study by Fawaz M. M. Mokbal et al. [5] overview one of the most important defenses against cybersecurity assaults is an IDS that employs the Al method. Nonetheless, there is always work to be done to increase IDS accuracy, detection rate, and minimize false alarm. The performance of such systems is strongly dependent on the quality and dependability of the training dataset. Through the use of an embedded feature

selection method and the most recent machine learning methodology, XGBoost, our research generated cutting-edge and complex cyber-defense strategies. Additionally, the most uniform feature subset for every attack is retrieved using the most recent real-world intrusion dataset, CICIDS2017. In comparison to other recently presented methods for solving intrusion detection issues, our suggested detection framework proved to have strong advantages, benefits, and the capacity to be incredibly competitive with an accuracy rate of 99.86%. In 2022 Zakaria Suliman Zubi [4] illustrated that the creation of sophisticated intrusion detection systems (IDSs) was suggested by this study project in an effort to reduce the quantity of false alarms that are created. Both false positives and false negatives increase network security and boost the detection rate of various assault types. Using the MATLAB program, the Naive Bayesian method was applied to the built-in intrusion detection systems (IDSs) in various scenarios. A comparative analysis between the IDSs and prior methods was then carried out, with an emphasis on analyzing performance parameters and identifying the most effective statistical technique for identifying different kinds of intrusions [6]. The performance of the implemented systems was evaluated using the NSL-KDD database, which consists of 41 network connection attributes. Experiments employing the NSL-KDD data set are used to gauge the effectiveness of the IDS. According to the Naive Bayes classifier results, the best IDS detection rate utilizing HTTP service is around 88.1643%. The false-negative rate is approximately 11.8357%, and the false-positive rate is approximately 0.6.60%. Mavra Mehmood et al. [7] shows that NSLKDD dataset is used in this study to project a detection system using data transformation, maximizing, and minimizing techniques. The NSLKDD dataset is divided into two classes using FGSVM: attack class and normal class. Significant findings from FGSVM indicate that 99.03% of samples can identify DDOS, probe U2R, and R2L. Through ANFIS, aberrant patterns found by FGSVM are activated. ANFIS selects five features for training, testing, and validation based on their importance scores and prediction roles. Epochs and error tolerance are defined between 0 and 100. The MSE is 0.08523 during training and 0.08496 during testing and validation. These values indicate respectable accuracy rates for the accurate identification of DDOS, Probe, R2U, and U2R The 2022 work done by Bhushan Deore et al. [8]. Here, an effective and reliable network ID technique called DASObased Deep RNN is presented to identify unusual activity in the background of network traffic. After being collected by the database, the pre-processing section receives the network traffic statistics and converts the raw data into sampled data. The pre-processed data is then handed over to the feature selection stage, where the Bayesian information gain model is used to efficiently identify the important and relevant features [9]. The naive bayes classifier, which is based on the IG, mutual information, and CIG, is used in the Bayesian information gain model. The Deep RNN classifier determines if the traffic behavior is normal or abnormal using the features that have been chosen [10]. The suggested DASO technique is used to train the Deep RNN classifier. The DE and ASO, respectively, are added to create the suggested DASO system [11]. Weights are improved by the suggested DASO system that makes use of the fitness measure [12]. Using the BoT-IoT dataset, the suggested DASO produced wellpresented metrics for accuracy, specificity, and sensitivity, with corresponding values of 0.9867, 0.8494, and 0.9988. Future research could improve the intrusion detection approach's presentation by utilizing a different optimization algorithm.

The 2020 work of Jesus Arturo Perez-Diaz et al. [21] presents a flexible modular architecture designed for identification and mitigation of Low-Rate Distributed Denial of Service (LR-DDoS) assaults, in response to the ongoing issue of mitigating them, especially in SoftwareDefined Networking (SDN) environments. An Intrusion Detection System (IDS) trained with six machine learning modelsJ48, Random Tree, REP Tree, Random Forest, Multi-Layer Perceptron (MLP), and Support Vector Machines (SVM) is incorporated into the design. Even with the inherent difficulties in identifying LR-DDoS attacks, the suggested technique obtains an amazing 95% detection rate through evaluation utilizing the Canadian Institute of Cybersecurity (CIC) DoS dataset. By using a Mininet virtual machine running the Open Network Operating System (ONOS) controller, the deployment ensures a simulation environment that closely resembles actual production networks.

In 2012 work of Sathishkumar et al. [30] presents data availability, data replication, data diffusion are the important issues to focus on networks. The proposed gauss Markov mobility model performed better in terms of partition stability and data storage capacity.

The study sought to build a broad range of network traffic data, spanning both legal and illegal behavior, using data from Kaggle. Numerous unauthorized access attempts and network attacks, such as probing, are included in the collection [13]. This large dataset can be used to evaluate and train the proposed method to effectively detect and classify different types of network intrusions [14]. The use of actual network traffic data from Kaggle ensures the robustness and dependability of the intrusion detection system [15]. As a result, the system is better able to recognize and eliminate possible threats in network environments.

3. MATERIALS AND METHODS

The security of computer networks and systems is critical in today's networked digital environment. Organizations constantly confront a threat to their sensitive data, vital infrastructure, and operational continuity due to the sophistication and frequency of cyberattacks [16]. In order to detect and stop malicious activity and unauthorized access, IDS monitor network traffic and system operations. This is a critical part of their defense against these threats [17]. Conventional IDS methods use signature-based or rule-based systems to find patterns of known attacks. Although somewhat successful, these techniques frequently fail to identify

new or undiscovered risks [18]. An increasing number of people are interested in using neural network topologies, like RNNs and LSTM networks, for intrusion detection as a result of the development of deep learning technology [19]. Because RNNs and LSTMs are good at modelling sequential data, time-series network traffic data analysis can benefit greatly from their use [20]. Deep learning-based IDS possess the capability to autonomously learn and adjust to changing attack tactics and network phenomena, in contrast to conventional IDS techniques that could depend on manually created rules or signatures. The process begins with data pre-processing to training and ends with deployment. Now a days AI based Machine learning and deep learning models are widely used in health care to diagnose several diseases [29].

3.1 PROPOSED MODEL

The suggested solution provides a comprehensive framework intended to overcome the built-in shortcomings of conventional IDSand enhance their capabilities. Recognizing that IDS are essential security tools for keeping an eye on networks traffic, the system uses deep learning techniques to improve threat detection accuracy by extracting useful insights from the complex data landscape. In order to mitigate the limitations associated with a purely deep learning approach, the framework presents a novel hybrid algorithm that makes use of a calculated blend of different machine learning techniques. The advantages of each technique are combined in this hybrid approach to produce an intrusion detection system that is more resilient and flexible. To further improve intrusion detection accuracy, the suggested system also uses feature engineering approaches. The system grows increasingly proficient at recognizing established attack patterns as well as abnormalities by extracting and honing pertinent elements from network data. This Dual capability improves the system's overall efficacy in defending systems and networks against a variety of cyberthreats. Notably, the framework's hybrid algorithm which combines BiLSTM and RNN offers a complex and reliable solution.

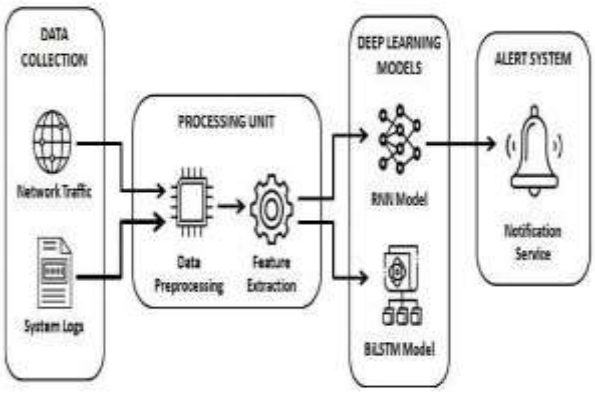

Fig 1: An Architecture Diagram for the Proposed Model

The goal of this all-encompassing strategy is to develop an increasingly sophisticated (IDS) that can identify a wider variety of threats, including both unusual and well-known patterns. Although the proposed architecture diagram's specifics are not given, it is clear from the context that it includes important components to improve the capabilities of the conventional IDS. Most likely, the architecture consists of parts of the data acquisition system, which records and processes network traffic. The hybrid algorithm intentionally incorporates deep learning techniques, specifically RNN and BiLSTM, to derive significant insights from the intricate data environment. The suggested architecture introduces a thorough framework to address the shortcomings of conventional IDS. The hybrid algorithm, which combines different machine learning techniques, is a key element that enhances the resilience and adaptability of the system. By fine-tuning the features that are retrieved from network data, feature engineering approaches let the system more precisely detect anomalies as well as recognized attack patterns. Real-time mechanisms are probably included in the architecture. To guarantee that the system is adaptable to changing cyber threats, monitoring, model updates, and retraining are required.

3.2 DATASET

The dataset is a crucial component of this project since it impacts the model's ability to generalize detection at different stages. A representative sample of both normal and anomalous data will be carefully chosen from the dataset to ensure a comprehensive and trustworthy training process. The NSL-KDD dataset, which is obtained from Kaggle, is a fundamental tool for assessing intrusion detection systems. It reflects the complexity of real-world network environments by encompassing a wide range of network traffic data, including both typical and unique sorts of attack situations. The dataset's carefully selected characteristics and annotated examples enable reliable model training and assessment, enabling researchers to assess intrusion detection algorithms' efficacy in a range of circumstances. Furthermore, the comprehensive documentation and standardised format

of the tool facilitate the data pre treatment and feature engineering processes, freeing up researchers to concentrate on the essential elements of model creation. Furthermore, the extensive use of the NSL-KDD dataset in both academia and industry promotes benchmarking and collaboration, which propels ongoing breakthroughs in intrusion detection research. Overall, its value as a benchmark dataset is immense, acting as a foundation for the creation and verification of cuttingedge intrusion detection methods meant to strengthen cyber defense against new and emerging threats.

3.3 PRE-PROCESSING

The first stage of getting the raw data ready and cleaned up to make it more suitable for analysis and modelling is called pre-processing. This usually entails a number of crucial activities, including feature selection, dataset balance, normalization, and data cleansing. Removing any errors, inconsistencies, or missing values from the dataset is known as data cleaning. By ensuring that all features have a same scale, normalization helps to avoid specific features from overpowering the analysis because of their greater size. In feature selection, the most pertinent features that greatly aid in the detection of network intrusions are found and chosen, with redundant or unnecessary features being removed. Several important pre-processing processes are carried out in order to prepare the dataset for training RNN and BiLSTM models for intrusion detection. The dataset is first gathered, which includes data related to system operations and network traffic. Data cleaning techniques are then applied to deal with any missing values and outliers that can have an impact on the performance of the model. Next comes feature selection, in which pertinent features are picked in order to successfully capture patterns suggestive of intrusion attempts. Normalization is applied to numerical features to ensure uniform scaling throughout the dataset, and numerical representations are encoded into categorical variables to comply with model specifications. Following that, temporal data is combined into fixed-length sequences designed specifically for RNN and BiLSTM architectures. The dataset is divided into separate training, validation, and test sets in order to guarantee reliable model training. To improve the dataset's diversity and balance, strategies like data augmentation and class imbalance treatment may be used. In order to guarantee consistent length for input sequences and enable a smooth integration into the model training procedure, sequence padding is finally implemented. The basis for developing strong intrusion detection systems that can successfully detect and mitigate security threats in network environments is laid by this methodical data preparation procedure.

3.4 MODEL CREATION AND PREDICTION

The initial stage in creating and predicting models with RNN and BiLSTM is to define the neural network's architecture. The number of hidden layers, the number of units or neurons in each layer, the activation function (such as tanh or ReLU), and the input data's sequence length are important parameters for RNNs. Other crucial LSTM parameters are the learning rate for optimization, the dropout rate to avoid overfitting, and the number of memory cells, or units, within each LSTM cell. The model is trained using historical data from the Kaggle network intrusion detection dataset after the architecture has been established. The model gains the ability to recognize patterns and temporal dependencies in the network traffic data during training.

A. BIDIRECTIONAL LONG SHORT TERM MEMORY

Using BiLSTM networks in an IDS is a powerful way to strengthen cyber security defenses against networkbased threats. BiLSTMs are effective at modeling the complex patterns seen in network traffic because of their bidirectional processing, which allows them to capture temporal dependencies within sequential data. In actuality, this means encoding and converting unprocessed network data into a format that is appropriate for the BiLSTM model. To distinguish between normal and anomalous behavior, the bidirectional LSTM cell model is trained on labeled network traffic data. The trained model assesses incoming network sequences in real-time during inference, looking for variations from ingrained patterns that can indicate possible security lapses. Standard criteria are used to assess the BiLSTM-based IDS's performance, and regular fine-tuning guarantees that it can react to changing threats. After it is installed, the intrusion detection system (IDS) blends in well with the current network architecture, adding another line of protection and strengthening the overall cyber security posture. The BiLSTM-based IDS makes a substantial contribution to the proactive detection and mitigation of security threats in dynamic network settings thanks to its sophistication and adaptability.

B. RECURRENT NEURAL NETWORKS

IDS, RNNs have become a powerful tool, especially because of their ability to handle sequential data that is present in network traffic. Because of their recurrent connections, RNNs are able to identify patterns of both benign and possibly harmful behavior across time by capturing temporal relationships within the data. The ability of RNNs to learn representations directly from unprocessed network traffic data eliminates the need for hand-crafted features, which is one of its main advantages. The capacity to learn features is what enables RNN-based intrusion detection systems to independently adjust to changing threats. Furthermore, RNNs make real-time intrusion detection easier, guaranteeing prompt reactions to security risks as they materialize. Because of their adaptability, they can be used with other machine learning strategies to improve detection accuracy and resistance to complex threats. As a result, RNNs have great potential for strengthening cyber security defenses by offering proactive and flexible solutions to a wide range of network-based threats.

3.5 FEATURE EXTRACTION

In the domain of network intrusion detection, feature extraction entails turning unprocessed data from the publicly available Kaggle dataset into a set of discriminative and significant features that effectively capture pertinent details about network traffic patterns. Statistical, structural, or frequency-based properties are often extracted from the network packets or flows during this procedure. Measures like the mean, standard deviation, skewness, and kurtosis of the packet size or inter-arrival periods are examples of statistical features. Extraction of data regarding the protocol type, source and destination IP addresses, port numbers, and packet flags may be necessary for structural characteristics. The incidence rates of particular network protocols or communication patterns within a specified time span may be captured using frequency-based characteristics. An essential step in intrusion detection systems (IDS) is feature extraction, which turns unprocessed network data into readable representations that help with categorization and analysis. First, pertinent traits are chosen or designed with the intention of separating malevolent from legitimate network activity using their discriminative power. After that, dimensionality reduction strategies are used to lessen the computational load and any overfitting brought on by high-dimensional data. Features collected from network traffic data include statistical metrics, time series traits, packet-level details, and session-level characteristics. These characteristics encompass a range of network communication patterns, such as protocol distribution, traffic volume, and anomalous behavior.

A. MODEL TRAINING

RNN and BiLSTM networks are used in IDS training. This is a methodical procedure that successfully separates possibly harmful activity from regular network behavior. The network traffic data is first preprocessed to remove noise and transform it into an appropriate format. Training and testing sets are frequently created from this procedure. After that, pertinent features are extracted to capture important aspects of network traffic, allowing the model to pick up discriminative patterns.The RNN or BiLSTM model's architecture is painstakingly created; in the case of the BiLSTM, bidirectional links are included to fully represent temporal dependencies. Labeled data is supplied into the model during training, and iterative adjustments are made to its parameters using optimization procedures such as stochastic gradient descent. In order to avoid overfitting and guarantee strong generalization, the model's performance is assessed concurrently using validation measures. The process of hyperparameter tuning refines the model's setup even further, leading to the identification of the top-performing model for ultimate testing dataset evaluation. By taking such a strict approach, the trained IDS is guaranteed to detect intrusions in actual network traffic, strengthening cybersecurity defenses against dynamic threats.

3.6 PERFORMANCE METRICS

The work presents a unique method of identifying anomaly by combining the Intrusion Detection System model with the RNN and BiLSTM algorithms. This combination works quite well and is a potential approach to the accurate identification of anomaly. Future research may go into supplementary RNN and BiLSTM models in various techniques. With precision, recall, and F1 score acting as performance indicators, the proposed method notably attains an impressive accuracy of 96.3%.

The formula for calculating Accuracy, Recall, F1- score and Precision

A. Accuracy: Accuracy is defined as the proportion of accurately identified occurrences both actual positives and true negatives—across all examples in the dataset. Although accuracy is a crucial criterion, it might not be enough for datasets that are unbalanced, such those used in jobs involving medical diagnosis.

$$\text{Accuracy} = (TP+TN) / (TP+TN+FP+FN) *100 \quad (1)$$

B. Precision: According to its definition, precision is the percentage of accurately anticipated positive outcomes among all of the beneficial projections the model produces. Regarding the prognosis of breast cancer, precision measures how well the model identified malignant cases among all the cases it has classified as such. A low rate of false positives is indicated by a high precision in the model.

$$\text{Precision} = (TP) / (TP+FP) *100 \quad (2)$$

C. Recall: Recall metric quantifies the percentage of real positives, or intrusions, that the IDS correctly detects. A high recall shows that the majority of intrusions are successfully captured by the IDS, whereas a low recall implies that many intrusions are going unnoticed.

$$\text{Recall} = (TP) / (TP+FN) \quad (3)$$

D. F1-score: A statistic that assesses how well memory and accuracy are equal is called the F1-Score. It is computed using the integrated mean of precision and recall. When there is a disparity in the dataset's classes, it is especially helpful. An improved balance between recall and precision is indicated by a higher F1-Score.

$$\text{F1 Score} = 2 * (TP)/(2TP+FP+FN) *100 \quad (4)$$

4. EXPERIMENTAL RESULT

For efficient evaluation, make sure the dataset is formatted and labelled correctly and is divided into distinct training and testing sets. In case training is required, handle missing values, choose pertinent features, and

properly prepare the data. Adapt the model based on the training set. Analyse the model's performance with testing sets, calculating metrics such as ROC curve, F1-score, recall, accuracy, and precision.

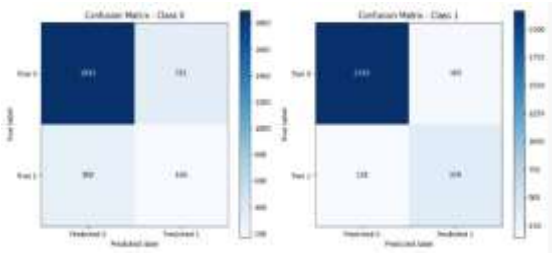

Fig 2: Confusion Matrix

Prior to testing, prepare training data for testing by executing pre-processing tasks such as normalization and sequence generation. To find out if an anomaly exists in the provided dataset, load a hybrid RNN and BiLSTM model after training an RNN model to detect anomalies. Use metrics like accuracy, ROC curve, F1-score, precision, recall, and F1-score to compare the predicted labels with the ground truth in order to evaluate the model's performance or when various error types have inconsistent consequences. They provide insights into the benefits and drawbacks of the model, which help guide future optimization and decision-making. A confusion matrix, shown in fig. 3, is commonly used to evaluate the performance of a classification model. It provides performance metrics for machine learning algorithms by contrasting normal and anomaly classes. A confusion matrix typically consists of four main components: True Positives (TP): Situations in which an incursion is accurately detected by the IDS. True Negative (TN): Situations in which regular network traffic is accurately classified as non-intrusive by the IDS. False Positive (FP): When an intrusion detection system (IDS) mistakenly reports legitimate network activity as intrusive (false alert). False Negative (FN): Situations in which a real incursion is not detected by the IDS. Confusion matrices are helpful instruments for evaluating the performance of a classification model, particularly in scenarios where there can be imbalances between the classes or when various error types have inconsistent consequences.

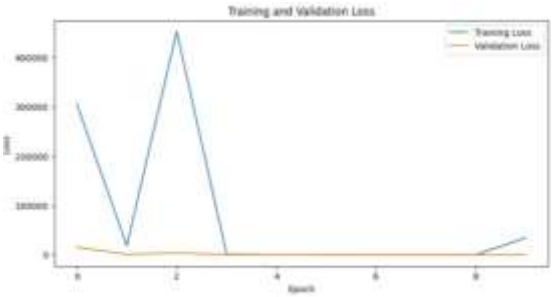

Fig 3: Training and Validation Loss

It is critical to monitor validation loss as well as testing loss when using IDS that uses RNNs and BiLSTMs. It guarantees the effectiveness of the system in identifying anomalies in practical situations while preserving generalizability in a variety of network setups. Through the utilization of these loss data, stakeholders can improve the capabilities of the IDS in an iterative manner, strengthening network defenses against dynamic attacks. Modern IDS solutions provide security analysts with actionable insights to efficiently reduce cyber risks by focusing on interpretability and explainability and making large-scale tagged datasets available. Deep learning techniques and real-world deployment situations are being explored further, which could lead to even more advanced intrusion detection systems in the future. These systems would be able to protect network infrastructures from an increasingly diverse range of cyber threats. Furthermore, by integrating with already-existing network security infrastructure and utilizing online learning and adaptation tools, these systems may dynamically change and adjust in real-time to everchanging threat environments

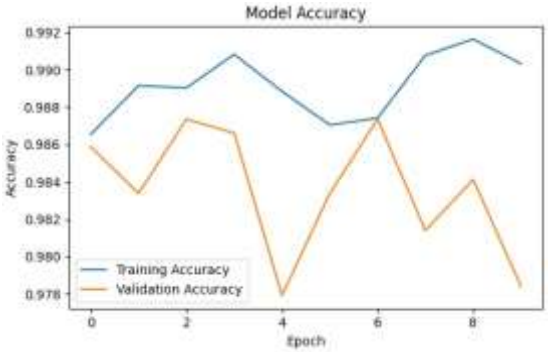

Fig 4: Model Accuracy

They provide insights into the benefits and drawbacks of the model, which help guide future optimization and decision-making

Table 1: Performance of DL Algorithm

Model	Accuracy	Precision	Recall	F1- score
Convolutio nal Neural Network (CNN)	91.96%	93.76%	92.67%	85.94%
Multilayer perception Model (MLP)	90.89%	91.22%	93.91%	94.06%
Group-ABC	94.4%	92.11%	84.47%	93%
RNN and BILSTM	96.3%	96.83%	98.1%	97.5%

Convolutional Neural Network (CNN): With an accuracy of 91.96%, the CNN is able to classify around 91.96% of the dataset's instances correctly. The CNN maintains a low incidence of false positives while exhibiting a high degree of accuracy in spotting intrusions, with a precision of 93.76%. With a recall rate of 92.67%, it demonstrates how well it can distinguish genuine invasions from the good ones. The F1-score of 85.94% strikes a solid mix between recall and precision, indicating that CNN effectively manages the risk of false alarms while reliably identifying intrusions.

Multilayer Perceptron Model (MLP): With an accuracy of 90.89%, the Multilayer Perceptron Model (MLP) does well overall in classification. The MLP shows a high degree of accuracy in detecting intrusions with a precision of 91.22%, while keeping a low incidence of false positives. Its 93.91% recall rate indicates how well it can identify genuine incursions among the good ones. The MLP's balanced precision and recall performance is reflected in its F1-score of 94.06%, which shows that it can effectively identify intrusions while reducing false alarms.

Group-ABC: The Group-ABC model demonstrates its competence in classification tasks with an accuracy of 94.4%. The model maintains a low incidence of false positives while demonstrating a high degree of accuracy in spotting intrusions, with a precision of 92.11%. Nevertheless, its 84.47% recall rate suggests a reduced capacity to identify all genuine incursions amidst the favorable occurrences. Although there may be opportunity for growth in terms of more accurately detecting actual incursions, the F1-score of 93.0% indicates a balanced performance in terms of precision and recall.

RNN with BiLSTM: When it comes to classification tasks, the RNN with BiLSTM performs better than the other models, with the greatest accuracy of 96.3%.

The model shows a high degree of accuracy in detecting intrusions while keeping a low rate of false positives, with a precision of 96.83%. Its 98.1% recall rate demonstrates how well it can identify genuine intrusions among the favourable occurrences.

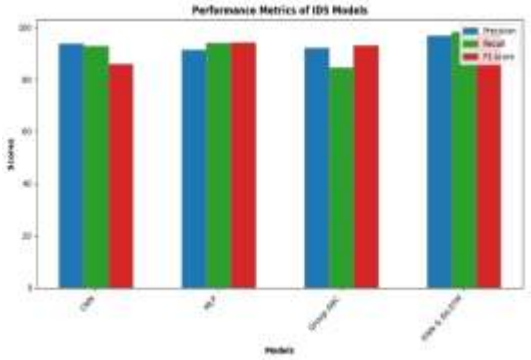

Fig 5: Graph represents the performance of various algorithms

The exceptional balance between recall and precision is reflected in the F1-score of 97.5%, which highlights the model's efficacy in precisely identifying intrusions while reducing false alarms.

5. STATE OF ART COMPARISON

Recent years have witnessed notable progress in the stateof-the-art for (IDS) that use (BiLSTMs) and Recurrent Neural Networks (RNNs). These models are very good at identifying both known and unknown threats because they are very good at capturing complex temporal correlations within network traffic data. Modern IDS systems based on RNNs and BiLSTMs exhibit resilience against evasion attempts and adversarial manipulations by utilizing advanced architectures.

Table 2: State of art comparison

	Method	Accuracy	Recall	F1-Score	Precision
Proposed Work	RNN and BiLSTM	96.3%	98.1%	97.5%	96.83%
Hakan Can Altunay, et al. (2023) [22]	CNN and LSTM	93.21%	93.1%	93%	92.99%
FatimaEzzahra Laghrissi, et al.(2021) [23]	LSTM	92.77%	96.62%	95.92%	94.23%
Pooja Shettar, et al.(2021) [24]	MLP and Chaotic NN	94.89%	95.91%	96.06%	91.22%
Xiaoxuan Zhang, et al.(2019) [25]	CNN	91.96%	94.67%	85.94%	91.76%
Nishika Gulia, et al.(2023) [26]	Group-ABC	93.4%	84.47%	94%	93.11%
Manish Kumar et al.(2012) [27]	Decision Tree	88.2%	87%	92%	94%
Mikel K. Ngueajio et al.(2022) [28]	Support Vector Machine	87.6%	89%	88%	87%

A comparative review of several intrusion detection techniques and the performance metrics that go along with them is shown in this table. RNN and bidirectional long short-term memory networks BiLSTM are the key components of the suggested method, which yields the maximum accuracy (96.3%), recall (98.1%), F1-score (97.5%), and precision (96.83%). While retaining competitive scores across other measures, current approaches that utilize CNN and LSTM networks exhibit marginally poorer accuracy at 93.21%. Furthermore,

recent studies by Pooja Shettar et al. and Fatima-Ezzahra Laghrissi et al. show encouraging outcomes with accuracies of 94.89% and 92.77%, respectively, as well as excellent performance in recall, F1-score, and precision. The CNNbased method of Xiaoxuan Zhang et al. obtains a reasonable accuracy of 91.96%, albeit with a 85.94% is the F1-score. Additionally, the Group-ABC technique by Nishika Gulia et al. shows a balanced performance with competitive scores in recall, F1-score, and precision, and an accuracy of 93.4%. With accuracies ranging from 87.6% to 88.2%, older methods like Decision Trees and Support Vector Machines still offer insightful analyses of intrusion detection, even though their accuracy is lower than that of deep learning-based techniques. All things considered, these results highlight how deep learning techniques specifically, RNN and BiLSTM architectures can improve Intrusion Detection Systems' precision and dependability.

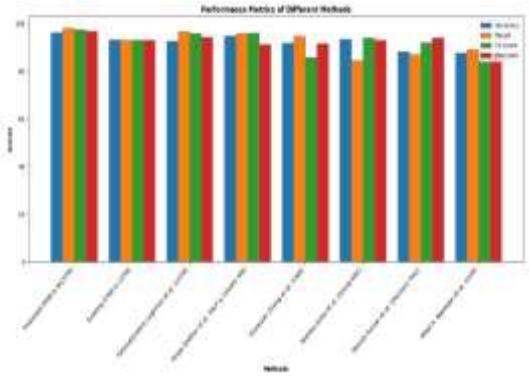

Fig 6: Performance Metrics

5. CONCLUSION

Combining RNN and BiLSTM algorithms with conventional machine learning techniques is a promising advance in network intrusion detection. The proposed system demonstrates better robustness and improved performance in distinguishing between benign and malicious activity by effectively extracting temporal relationships from network data and utilizing feature engineering to improve precision.. In today's dynamic cybersecurity world, the framework demonstrates its potential to detect changing risks and provides superior defences against sophisticated cyber threats through thorough assessments on public datasets. Prospective research endeavours may concentrate on augmenting the framework's scalability and adaptability to nascent cyber threats by the investigation of sophisticated deep learning architectures and the integration of real-time anomaly detection methodologies. To further enhance the detection and mitigation capabilities of intrusion detection systems, research could also focus on integrating contextual data and utilizing outside threat intelligence sources. Additionally, researching the use of reinforcement learning algorithms for intrusion detection system optimization and dynamic adaptation may provide insightful information about how to create more proactive and resilient defences against changing cyber threats.

REFERENCES

1. Nishika Gulia, Kamna Solanki, Sandeep Dalal, Amita Dhankhar, Omdev Dahiya, N. Ummal Salmaan, "Intrusion Detection System Using the G-ABC with Deep Neural Network in Cloud Environment", Scientific Programming, vol. 2023, Article ID 7210034, 15 pages, 2023. https://doi.org/10.1155/2023/7210034
2. Hossain, Md & Ghose, Dipayan & Partho, All & Ahmed, Minhaz & Chowdhury, Md Tanvir & Hasan, Mahamudul & Ali, Md & Jabid, Taskeed & Islam, Maheen. (2023). Performance Evaluation of Intrusion Detection System Using Machine Learning and Deep Learning Algorithms. 1-6. 10.1109/IBDAP58581.2023.10271964.
3. T. Sowmya, E.A. Mary Anita, A comprehensive review of AI based intrusion detection system, Measurement: Sensors, Volume 28, 2023, 100827, ISSN 2665-9174, https://doi.org/10.1016/j.measen.2023.100827.
4. Zubi, Zakaria & Ibrahim, Abdul. (2022). Use of Naive Bayesian Filtering in the Intrusion Detection System (IDS). International Journal of Circuits, Systems and Signal Processing. 16. 831-842. 10.46300/9106.2022.16.102.
5. Mokbal, Fawaz & Dan, Wang & Osman, Musa & Ping, Yang & Alsamhi, Saeed. (2022). An Efficient Intrusion Detection Framework Based on Embedding Feature Selection and Ensemble Learning Technique. The International Arab Journal of Information Technology. 19. 10.34028/iajit/19/2/11.
6. Mokbal, Fawaz & Dan, Wang & Osman, Musa & Ping, Yang & Alsamhi, Saeed. (2022). An Efficient Intrusion Detection Framework Based on Embedding Feature Selection and Ensemble Learning Technique. The International Arab Journal of Information Technology. 19. 10.34028/iajit/19/2/11.

7. Mehmood, Mavra & Javed, Talha & Jamel, Nebhen & Abbas, Sidra & Abid, Rabia & Bojja, Giridhar & Rizwan, Muhammad. (2021). A Hybrid Approach for Network Intrusion Detection. Computers, Materials & Continua. 70. 10.32604/cmc.2022.019127.
8. Deore, Bhushan & Bhosale, Surendra. (2022). Intrusion Detection System with a Modified DASO Optimization Algorithm. International Journal on Engineering, Science and Technology. 4. 2022. 10.46328/ijonest.66.
9. A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A new ensemble-based intrusion detection system for Internet of Things," Arabian J. Sci. Eng., vol. 47, pp. 1–15, Aug. 2021.
10. A. A. Aburomman and M. B. Ibne Reaz, "A novel SVM-kNN-PSO ensemble method for intrusion detection system," Appl. Soft Comput., vol. 38, pp. 360–372, Jan. 2016.
11. Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Trans. Emerg. Telecommun.Technol., vol. 32, no. 1, p. e4150, Jan. 2021.
12. Ahmim, M. Derdour, and M. A. Ferrag, "An intrusion detection system based on combining probability predictions of a tree of classifiers," Int.J. Commun. Syst., vol. 31, no. 9, p. e3547, Jun. 2018.
13. M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," IEEE Access, vol. 6, pp. 52843–52856, 2018.
14. K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in Proc. 15th IEEE Int. Conf.Mach. Learn. Appl. (ICMLA), Dec. 2016, pp. 195–200.
15. Alsughayyir, A. M. Qamar, and R. Khan, "Developing a network attack detection system using deep learning," in Proc. Int. Conf. Comput.Inf. Sci. (ICCIS), Apr. 2019, pp. 1–5.
16. G. Andresini, A. Appice, N. D. Mauro, C. Loglisci, and D. Malerba, "Multi-channel deep feature learning for intrusion detection," IEEEAccess, vol. 8, pp. 53346–53359, 2020.
17. R. A. R. Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He, "Fuzziness based semi-supervised learning approach for intrusion detection system," Inf. Sci., vol. 378, pp. 484–497, Feb. 2017.
18. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun.Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.
19. L. Buschlinger, R. Rieke, S. Sarda, and C. Krauß, "Decision tree-based rule derivation for intrusion detection in safety-critical automotive systems," in Proc. 30th Euromicro Int. Conf. Parallel, Distrib.
20. NetworkbasedProcess. (PDP), Mar. 2022, pp. 246–254. K. A. Da Costa, J. P. Papa, C. O. Lisboa, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," Comput. Netw., vol. 151, pp. 147–157, Jan. 2019.
21. M. A. Jabbar, R. Aluvalu, and S. S. Reddy S, "RFAODE: A novel ensemble intrusion detection system," Proc. Comput. Sci., vol. 115, pp. 226–234, 2017.
22. Hakan Can Altunay, Zafer Albayrak, A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks, Engineering Science and Technology, an International Journal, Volume 38, 2023, 101322, ISSN 2215-0986, https://doi.org/10.1016/j.jestch.2022.101322.
23. Laghrissi, F., Douzi, S., Douzi, K. et al. Intrusion detection systems using long short-term memory (LSTM). J Big Data **8**, 65 (2021). https://doi.org/10.1186/s40537-02100448-4
24. P. Shettar, A. V. Kachavimath, M. M. Mulla, N. D. G and G. Hanchinmani, "Intrusion Detection System using MLP and Chaotic Neural Networks," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9457024.
25. X. Zhang, J. Ran and J. Mi, "An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic," 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 2019, pp. 456-460, doi:10.1109/ICCSNT47585.2019.8962490.
26. Nishika Gulia, Kamna Solanki, Sandeep Dalal, Amita Dhankhar, Omdev Dahiya, N. Ummal Salmaan, "Intrusion Detection System Using the G-ABC with Deep Neural Network in Cloud Environment", Scientific Programming, vol. 2023, Article ID 7210034, 15 pages, 2023.
27. M. Kumar, M. Hanumanthappa and T. V. S. Kumar, "Intrusion Detection System using decision tree algorithm," 2012 IEEE 14th International Conference on Communication Technology, Chengdu, China, 2012, pp. 629-634, doi: 10.1109/ICCT.2012.6511281.
28. Ngueajio, Mikel & Washington, Gloria & Rawat, Danda B & Ngueabou, Yolande. (2022). Intrusion Detection Systems Using Support Vector Machines on the KDDCUP'99 and NSL-KDD Datasets: A Comprehensive Survey. 10.1007/978-3-031-16078-3_42.
29. Sathishkumar, R., and M. Govindarajan. "A Comprehensive Study on Artificial Intelligence Techniques for Oral Cancer Diagnosis: Challenges and Opportunities." In 2023 International Conference on System, Computation, Automation and Networking (ICSCAN), pp. 1-5. IEEE, 2023.
30. R. Sathishkumar, S. Pariselvam, "Formative impact of Gauss Markov mobility model on data availability in MANET," Asian Journal of Information Technology, vol. 11(3), pp.108-116, 2012.