International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Intrusion Detection System Using Recurrent Neural Network-Long Short-Term Memory

Mr. Kishor P. Jadhav[1] Dr. Tripti Arjariya[2] Prof. (Dr.) Mohit Gangwar[3]

Submitted: 26/01/2023 **Revised:** 20/03/2023 **Accepted:** 16/04/2023

Abstract: To build an Intrusion Detection System (IDS) for identifying and categorising cyber-attacks in a prompt and autonomous manner both on the network and the host level, machine learning approaches are being utilized extensively. On the other hand, due to the fact that malicious attacks are always evolving and taking place in extremely high volumes, it is necessary to develop a solution that can be scaled up. The cyber security community has access to a variety of malware datasets that can be used for further research in the public domain. Furthermore, no study that is currently accessible has given a complete evaluation of the effectiveness of different machine learning techniques on different datasets that are publicly available. A form of hybrid deep learning model, Recurrent Neural Network-Long Short Term Memory (RNN-LSTM) is investigated in this paper with the goal of developing a flexible and effective intrusion detection system that can detect and classify unanticipated and unforeseen cyber-attacks using the datasets KDDCup99 and NSLKDD. The results of this type of study make it easier to select the optimal algorithm that has the potential to effectively work in identifying future cyber attacks. By using the KDDCup and NSLKDD datasets, a thorough analysis of experiments evaluating RNN-LSTM and other traditional machine learning classification models is shown. The abstract as well as high-dimensional feature representation of the intrusion detection system data is used to develop the RNN-LSTM model that was developed by feeding the features into a large number of hidden layers. Two experiments using binary and 5- group classification method has been performed, it is observed from these experiments that the performance of RNN-LSTM method based on binary classification is 83.29% and 68.59% using KDD Cup 99 and NSLKDD dataset which is better as compared to other conventional machine learning classifier and 5-group classification method.

Keywords: *Intrusion Detection system, Recurrent Neural Network, Long Short Term Memory, Deep Learning.*

1. Introduction

The significance of network security has been steadily rising in recent years alongside the proliferation of the use of computer networks across all spheres of human existence. The confidentiality, integrity, and availability (CIA) of the information carried by a network are the three primary components of its security. A network intrusion can be defined as any action that attempts to breach CIA or that works around the security systems of a network [1]. An intrusion detection system (IDS) is a form of security management platform that is used to identify intrusions on a network [2]. In today's world, an IDS is an essential component of any modern network security system. In most cases, an IDS will examine each arriving and departing data packet of a specific network to evaluate whether or not the packet contains any indicators of an intrusion. An IDS that has been thoughtfully developed will be able to recognise the telltale signs of the majority of intrusion operations and instantly react to them by adding entries to security logs or sending alerts.

Depending on the primary detection methods, IDS can be separated into two distinct categories: misuse and anomaly detection [3]. Knowledge-based detection method is used for the purpose of detecting misuse. In order to properly identify an intrusion, a misuse detection system must first precisely specify the characteristics of the intrusion and then compare those characteristics to the rules. The identification of misuse can attain a high level of accuracy while maintaining a low percentage of false positives. On the other hand, it requires the construction of a feature collection and is unable to identify unknown attacks. Anomaly detection, on the other hand, is a behavior-based approach to detection methods. First, it must establish what the typical operations of a network are, and then it must determine whether or not the current behaviour has departed from the typical operations. Without having any prior information on an intrusion, outlier detection merely requires the typical state of a particular network to be defined. As a result, it is able to identify previously unknown forms of attack, despite the possibility of a high proportion of false positives. IDSs are facing an

[1]Ph.D. Research Scholar, Department of Computer Science and Engineering, Bhabha University, Bhopal, Madhya Pradesh, India
[2]Head, Department of Computer Science and Engineering, Bhabha University, Bhopal, Madhya Pradesh, India
[3]Director (Alumni Cell), B. N. College of Engineering and Technology, Lucknow
[3]mohitgangwar@gmail.com

increasing number of obstacles as a result of the ever-increasing complexity of network structures, as well as the diversification and complexity of the methods used by cybercriminals to launch intrusions.

There have been several investigations on machine learning that have led to the development of solutions that use machine intelligence to identify intrusions [18, 19]. In the realm of intrusion detection, for example, successful applications include the genetic algorithms, support vector machine (SVM) and artificial neural networks (ANNs). The straightforward approach to machine learning, on the other hand, has a number of drawbacks, whereas intrusion is growing increasingly intricate and diverse. It is necessary to improve learning approaches, particularly with regard to the automatic extraction and investigation of intrusion features. Deep learning (DL) has been the subject of extensive research and has proved very successful in the process of natural languages, the recognition of images, and the prediction of the weather [16, 17]. The models that are used in deep learning contain a high level of non-linear structure, which demonstrates exceptional learning power for the interpretation of complex information. DL is a subfield of machine learning. In addition, deep learning techniques now have a hardware base due to the rapid evolution of parallel computing that has taken place over the past few years [20, 21, 22, 23].

In the recent past, the Recurrent Neural Network, often known as an RNN, has been unsuccessful in becoming a popular network model due to the problems associated with training and the computation cost of the model [24, 25]. RNN has entered a phase of rapid progress in recent years, which coincides with the advancement of the theory of deep learning. In the present day, RNN has already been implemented with great success in hand gesture recognition and voice recognition. RNN's most notable characteristic is that it recirculates information in a hidden layer, which has the ability to store data that has been processed in the past. This provides a structural benefit for the analysis of time series data. In a similar fashion, numerous incursion behaviours are capable of being abstracted as particular time series of events originating from the network infrastructure. Therefore, RNN is a viable option for the construction of an IDS.

Therefore, RNN is a viable option for the construction of an IDS that is based on deep neural networks in order to increase both the cognitive capacity of IDS and the effectiveness of its detection capabilities. In particular, a new intrusion detection system is demonstrated that is made up of recurrent neural networks that have both long and short term memories (RNN-LSTM). On the KDD 99 and NSL-KDD datasets, the proposed system was subjected to a comprehensive evaluation. Both of these datasets have seen extensive use in the research that has come before them, which provides us with the opportunity to compare performance side by side. The suggested system utilises a DNN, which eliminates the need for users to manually select their system's features. It makes a considerable impact in the amount of work that needs to be done by network professionals and has a beneficial outcome in the constantly shifting network environment that exists today.

The remaining parts of this work are structured into 5 sections. The research that are relevant are summarised in Section II. In Section III, the components and overall design of the proposed system are presented. These components were used to develop the system. In Section IV, the details of the investigation and the outcomes are presented. The suggested system is brought to a conclusion in Section V.

2. Literature Survey

In order to fully utilise the value of both current input and historical data, H. Yang et al. [1] presented a multi-layer attention mechanism-based ID approach for power network systems. This approach seperates feature extraction into two distinct attention tiers at the feature and slice level. The intrusion detection methodology put forward in this study, according to experiments, increases detection accuracy while costing less, hence enhancing the reliability of the power information network.

The Network Intrusion Detection-Recurrent neural network (RNN) strategy for combining NID with Long Short Term Memory is described by S. Amutha et al. [2]. (LSTM). The method is tested utilising various activation function situations for NID on the one side, and the quantity of repetitions for BP on the other hand. The effectiveness of the suggested model relying on both multiclass and binary categorization is assessed using the UNSW-NB18 datasets. The test findings demonstrate that, in order to achieve the highest accuracy with a minimal amount of iterations, the efficiency of the suggested RNN was raised by roughly 8% when compared to the current RNN technique.

Recurrent Neural Network (RNN)-based NIDS with a multi-classifier to provide a detection approach in real time are proposed by K. Yu et al. in [3]. The proposed method intelligently and flexibly modifies the created model using the system characteristics that can be utilised as security factors to block real-time obscuring attacks from the attacker. According to the experimental findings, the suggested system identifies intrusion attempts with high precision and real-time model upgrades at fast speeds while demonstrating resilience to an attack.

In order to develop a model for a hybrid IDS, A. Halbouni et al. [4] took advantage of the capability of the Convolutional Neural Network to derive spatial characteristics and of the capability of the LSTM Network to retrieve temporal features. In order to improve the model's overall results, batch normalisation and dropout layers have been added to the structure. The model had been trained on the WSN-DS, CIC-IDS 2017 dataset and UNSW-NB15 dataset. The training was dependent on the binary and multiclass classifications. The efficiency of the system is determined by the confusion matrix, which takes into account a variety of parameters for assessment, including accuracy, specificity, detection rate, F1 measure, and False Alarm Rate (FAR). Experiment findings that showed a high detection rate, good accuracy, and a comparatively small FAR confirmed the usefulness of the model that was proposed.

A deep learning-based IDS was proposed by V. Rajasekar et al. [5] to solve the problems of low accuracy as well as feature extraction. The application of the RNN is accompanied by three stages of preprocessing, which include the numerical conversion of the data, the normalisation of the data, and the balance of the data. It is able to accurately portray the flow of internet traffic and improves the ability to spot unusual occurrences. The proposed model is evaluated using a standard dataset that is open to the public, and the results demonstrate that it is superior to other possible comparison methodologies. The evaluation of the results of the suggested procedure reveals that the accuracy rate is 99.56 percent, the average TPR is 99.55 percent, and the average TNR is 99.32 percent.

An ensemble Deep Learning IDS is proposed by U. Mbasuva et al. [6] for the purpose of detecting DDoS assault traffic in SDNs. An ensemble model consisting of a Convolutional Neural Network (CNN), RNN and a Deep Neural Network is constructed using the proposed method. The effectiveness of the proposed method is compared to the effectiveness of existing systems. The results demonstrate the effectiveness of the proposed ensemble deep learning approach is superior to that of the ensemble CNN, RNN, and voting approaches.

A unique deep learning model for the detection of anomalies in Internet of Things networks utilising a RNN is proposed by I. Ullah et al. [7]. The aforementioned model for the identification of anomalies in IoT networks is implemented with the help of the LSTM, BiLSTM, and Gated Recurrent Unit (GRU) approaches. Because CNNs are able to examine input characteristics without discarding crucial pieces of data, they are especially well-suited for the process of feature learning. CNN and RNN were subsequently utilised in the development of a hybrid model for deep learning. In conclusion, a lightweight DL approach for binary classification that uses GRU, LSTM and BiLSTM based techniques has been developed. The IOT-DS2, IOT-23, NSLKDD, BoT-IoT, IoT-NI and MQTT dataset are used to validate the suggested deep learning algorithms. The multiclass and binary classifier that was developed attained high levels of precision recall, accuracy, and F1 measure when compared to the DL algorithms that are already in use

According to B. Budler et al. [9] the present landscape of cybersecurity must include the detection of network intrusions as an essential component. Researchers have made significant strides over the years in utilising the capabilities of machine learning to detect and thwart network threats. Recently, there has been a rise in interest regarding the potential applications of Deep Learning in the field of network intrusion detection. Furthermore, NIDS that have been built utilising DL techniques are now being evaluated using the obsolete KDD Cup 99 and NSLKDD datasets, neither of which are indicative of the network traffic that occurs in the actual world. Current evaluations of these methods on the more recent CSE-CIC-IDS2018 dataset fail to acknowledge the extreme class imbalance that exists in the dataset, which results to findings that are significantly skewed. This research offers deeper insights into the effectiveness of these designs in the classification of modern network traffic data by tackling this class imbalance and conducting an exploratory investigation of a DNN, CNN, and LSTM Network on the balanced dataset. The DNN displayed the best performance of the classifier, achieving the highest accuracy of 83.8% and Fl-Score of 84.4% while also achieving the less FAR of 2.7%.

H. Babbar et al. [10] investigates the role of Ml and DL in Software Defined-IDS in Intelligent Transportation Systems (ITS). The mathematical evaluation of current DL models were discussed and evaluate their outcomes based on a number of different metrics to determine which model provides the best outcomes for the current state of the art. According to the findings, enhanced RNN are the most effective method for the detection of SD-IDS assaults in both the data plane and the control plane.

R. Kavitha et al. [11] emphasizes on Deep IDS techniques and studies ways to produce better outcomes at various phases of the intrusion detection phase. Examine the deep learning techniques such as the DNN, CNN-LSTM and RNN in addition to that in order to reach the highest accuracy level and precision with the fewest number of repetitions possible. Focus on the demonstration of each model in two different classifications of categorization (binary and multi-class) using the authentic traffic dataset NSL-KDD. The outcomes of the tests demonstrate that the RNN is capable of accurately classifying types of malicious with a rate of 99.4%. In contrast, the accuracy that the CNN-LSTM model attained was 95.4%, whereas the accuracy that the DNN model obtained was 91.8%.

D. Ding et al. [12] proposes an IDS that is based on a Bi-directional Long Short-Term Memory (Bi-LSTM) network and also a sliding window approach was designed. Time series linear regression was utilized on the real vehicle-mounted text data set in order to evaluate the sliding window of the optimised time length. The 2-D input data sample set is produced using the established sliding window. Next, the BILSTM network is employed to learn the 2D data feature training classification model. Finally, the trained network approach is utilised to accomplish intrusion detection. In this investigation, four different data sets were utilised to test and validate the performance of the detection. When compared to the research methodologies that are currently in use, the detection performance of the four different data sets rose by an average of 5.35%, 3.8%, 2.05%, and 3.45% respectively.

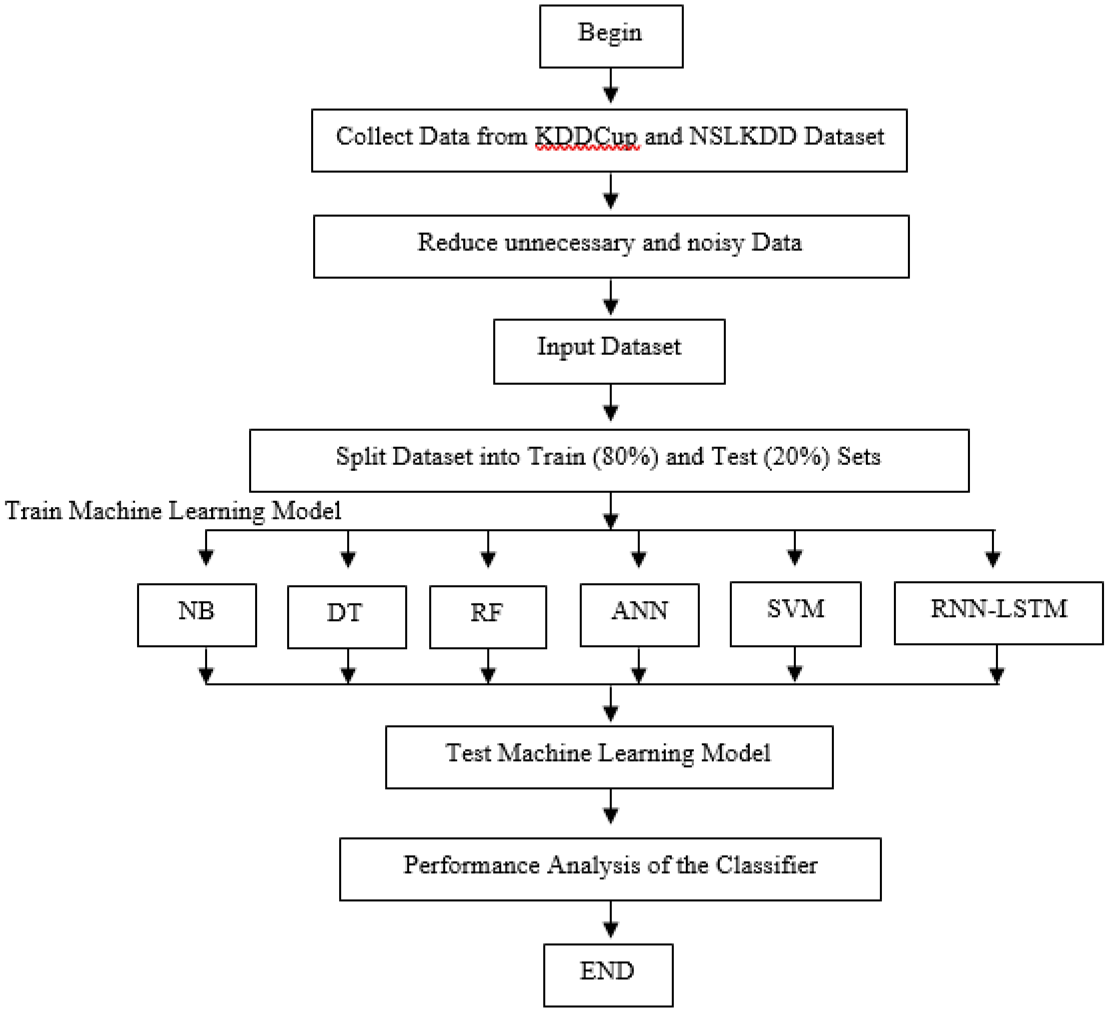
G. Ketepalli et al. [13] makes use of a straightforward LSTM autoencoder in conjunction with a Random Forest (RF) in order to identify potential intrusion attempts made by IDSs. In order to determine the extent to which this feature extraction method can improve accuracy, certain characteristics are enabled and disabled in turn. The NSL-KDD dataset has been utilised in order to determine whether or not detection methods are successful following the extraction of features. The two activation functions are contained within the autoencoder's hyper - parameters. The reliability rating of the losses and activation functions of the ReLU as well as the SoftMax is the highest among all functions. The primary objective of this research is to determine which features are the most useful by employing both a LSTM- Autoencoder and a RF. The preliminary results of experiments indicate that classifiers that make use of these parameters have a predictive performance of 94.74 percent.

The method of intrusion detection utilised by B. Deore et al. [14] is known as Chimp Chicken Swarm Optimization dependent Deep LSTM. In this scenario, the Deep LSTM is utilised for the purpose of accurately detecting invasion, and in order to improve the detection accuracy, the Deep LSTM is trained by employing a specific optimization strategy.

A novel IDS based on time series categorization and DL is proposed by Y. Yu et al. [15]. The time series of traffic parameters were gathered that are directly connected to traffic incidents from texts of automobiles that are located near observed traffic incidents as time - series data extracted features. This is done in light of the fact that traffic parameters have a strong correlation with the passage of time. A traffic incident classification model based on LSTM is created and trained utilising time series feature vectors from both regular and colluding attack circumstances. This allows for a more accurate recognition of the trend of traffic conditions that change over time. It is possible to ascertain whether or not the emergency message is genuine by looking at the classification performance. Lastly, an exhaustive simulation is used to evaluate the effectiveness of the LSTM-based intrusion detection system that was presented. The findings of the simulation demonstrate that the suggested intrusion detection system is more effective in the detection of bogus messages in comparison to several well-known ML-based techniques.

3. Research Methodology

Researchers in the field of information security have been inspired to implement a variety of machine learning strategies in recent years as a means of protecting organisations' data as well as their reputations in the face of the ever-increasing complexity and intensity of security attacks launched against computer networks. One of the existing methods, known as deep learning, has lately been utilised to a large extent by IDS, in order to improve the performance of these systems in terms of securing computer networks & hosts. By using datasets KDDCup99 and NSLKDD, the RNN-LSTM model has been used in the system that has been suggested in order to detect and categorise cyber-attacks that were neither predicted nor foreseeable. Take a look at figure 1, which presents a flowchart of the RNN-LSTM strategy that has been presented for detecting intrusions. Initially, the data is obtained from well-known datasets, KDDcup and NSLKDD. This data has been preprocessed in order to reduce the amount of noisy and superfluous data. The processed data is then divided into a train dataset consisting of 80% and a Test dataset consisting of 20% of data. This data is categorised by utilising a number of different traditional machine learning approaches and the proposed RNN-LSTM classifier. The detail description of each step of proposed approach is described as follows.



Begin
Collect Data from KDDCup and NSLKDD Dataset
Reduce unnecessary and noisy Data
Input Dataset
Split Dataset into Train (80%) and Test (20%) Sets
Train Machine Learning Model
NB
DT
RF
ANN
SVM
RNN-LSTM
Test Machine Learning Model
Performance Analysis of the Classifier
END

Fig. 1: Flowchart of Proposed RNN-LSTM for Detecting Intrusion

Data Collection: The best strategy to evaluate an intrusion detection system (IDS) is to use a standard dataset for testing, as this allows for a more objective evaluation of various systems. The KDD Cup 99 dataset has, over the course of many years, established for benchmarking due to its widespread use in the evaluation of IDSs. This dataset contains 39 different kinds of attacks, 22 of which are included in the training set, while the remaining 17 appear solely in the test set as unidentified attack types for the purpose of evaluating the algorithm's classification performance. Each of these assaults can be placed into one of these four categories:

- **Denial of Service (DOS):** blocking access to a service in order to hinder users from using it, example: syn flood.
- **Root to Login (R2L):** illegal access coming from a different computer, example: guessing password.
- **User to Root (U2R):** illegal access to privileges held at the local root level, example: buffer overflow.
- **Probe:** surveillance as well as other forms of investigating, example: port scanning.

In addition, taking into account the NORMAL state (where there have been no attacks), every record is categorised according to one of these five categories. Every connection record in KDDCup 99 contains a total of 41 characteristics, 34 of which are continuous and 7 of which are discrete-valued. All of the characteristics can be sorted into the following four major categories:

- The fundamental characteristics of each individual TCP connection. These characteristics are obtained by directly examining the packets' header information;
- Content-based derived features. Features of the content that are contained within a connection that is suggested by prior domain expertise;
- "same host" features. These features only look at connections that have been made in the previous two seconds and that use the same destination host as that of the current connection;

- "same service" features. These features only look at connections that have been made in the previous two seconds and have the same service as the current connection.

The NSL-KDD dataset addresses a number of the limitations of the KDD 99 database. To provide just one case, it does not contain any records that are redundant or duplicate. It is more suitable to choose a certain number of records from every degree of difficulty, which enhances the process of obtaining an accurate rating more effective. Because the total amount of records is appropriate, it is now possible to execute methods on the entire dataset rather than just on a small portion that is chosen at random. This opens up a lot of new possibilities. As a direct consequence of this, it is now much simpler to compare the findings of various investigations. For the purpose of assessing the suggested IDS in this research, the KDD 99 dataset as well as the NSL-KDD dataset were utilised. In each collection of data, the most frequently employed data files were chosen to ensure an accurate comparison.

Data Pre-Processing: Since the proposed system may take in only numerical inputs, it is crucial to convert any non-numerical data that may be included in the dataset into numeric values. The data formats of NSL-KDD and KDD 99 are identical since NSL-KDD is a modification of KDD 99. Within each record, there are just three aspects that are symbolized and have to be transformed to numerical data. These features are the protocol type, service, and flag. In order to achieve this goal, 1-to-N encoding will be utilised. In a similar fashion, the outcomes of the classification are expressed quantitatively (0 to K-1).

Feature Extraction and Selection: Using the training dataset as a preliminary step, a hybrid feature set is constructed by first collecting the five feature groups that are outlined as follows.

- **TF-IDF Features:** One of the features of TF-IDF is that it can determine the context of characteristic data based on phrases that appear frequently. The selection of features in several feature extraction techniques is dependent on either the numerical values of the attributes or the occurrence frequencies of the attributes.
- **Relational Features:** Projects involving text analysis and natural language processing make heavy use of these features. In an essence, relations are nothing more than a collection of values that coincide within a particular interval. This accomplishes a few different goals. Using these methods, it is possible to develop unigram models in addition to multiword models.
- **Auto-encoder Feature:** A neural network has the potential to develop efficient representations of the data by employing a method of unsupervised learning known as an autoencoder. In order for the network to acquire the necessary forms, this method instructs the network to ignore "noise" in the input. In the course of this research, while the RNN and LSTM are being executed, certain autoencoder features extracted and classified with the help of a hybrid classifier.
- **Attribute Relational File Format (.arff) Features:** It is a text file that has been written in ASCII and describes a group of instances that it all share the exact set of attributes in common. An ARFF file is composed of two portions that are entirely distinct from one another. The first part of the text is known as the Header information, and the second part, known as the Data, comes right after it. The introduction of the ARFF file contains a number of important pieces of information, including a list of the features and the types of those features, as well as the name of a particular relation.
- **Fuzzy Genetic Features:** During this feature extraction process, the various rules by utilising the Genetic Algorithm (GA) are extracted. When the GA execution is complete, it produces rules that are subsequently referred to as GA rules. When some data mining approaches, such apriori and fuzzy logic, are implemented to GA rules, the process ultimately results in the generation of association rules that are referred to as fuzzy genetic rules.

Classification: In this research, a wide variety of different classification models that were produced via machine learning were utilised. After computing every model's accuracy for the dataset that was given, the results are compared to the RNN-LSTM approach that was recommended. The following is a discussion of the conventional classification methods:

- **Decision Tree:** The Decision Tree technique is used to develop classification techniques in the area of machine learning [26]. This method to hierarchical classification is based on the form of a tree, which acts as the basis for the approach. This is an example of the type of learning known as supervised learning, which refers to circumstances in which the desired end result has been established in advance. The decision tree method is versatile enough to accept both sets of category data as well as sets of statistical information. The elements of a decision tree are the trunk, branches, and the many nodes at the ends of the branches. The data are evaluated according to the route that they followed to travel from the root node to any of the leaf nodes in the tree. The decision tree was used to analyse a total of 283 tuples as part of the procedure of generating decisions based on the dataset. Regarding the prediction of heart disease, it was probable that either a positive or unfavourable assessment would be made. When compared to the relevant parameters, the accuracy, selectivity, and sensitivity of the model were all assessed and evaluated.

- **Random Forest:** The random forest model is composed of a number of separate decision trees that function as a group; more precisely, each tree that makes up the random forest has a unique one-of-a-kind method of forecasting classes [28]. The Random Forest method is able to provide a higher amount of randomness and variety since it makes use of the bagging technique to the feature space. It does not conduct an exhaustive search for the most accurate predictors in order to produce branches; instead, it randomly samples elements of the predictor area. This leads to the furthermore of further wide range and a decline in the variance of the trees, despite the expense of a comparable or higher level of bias. "Feature bagging" is a powerful strategy that finally leads in a model that is significantly robust. The procedure is called "feature bagging."
- **Naive Bayes:** The statistical classifier, Naive Bayes functions under the premise that there is no link between the characteristics that are being taken into account. It does so by making an assumption about the value of a feature on a specific class, but it bases its conclusion about the independence of that conclusion on how the value in question correlates to the values of many other attributes. The concept behind this is called conditional independence [28].
- **Support Vector Machine (SVM):** It is a form of supervised learning that completes a task that is exactly equivalent to that of the C4.5 technique, despite the fact that it does not produce any utilization of decision trees [28]. SVM accomplishes this task by not using decision trees, which is the only difference between the two. The support vector machine undertakes an effort to cut down on the possibility of an inaccurate classification being assigned.
- **Artificial neural network:** Artificial neural networks were created largely for the purpose of computation when they were first invented. When compared to the traditional approach, this one has the overarching goal of reducing the amount of time necessary to finish a certain activity [29]. It is possible to draw parallels between the biological structure of neurons within the human brain and the depiction of that pattern in this model. In exactly the same way that neurons in the brain link to one another, neurons (also known as nodes) in this network will likewise link to each other. This representation consists of a very high number of neurons, all of which are linked each other and collaborate in order to carry out a specific task. Due to the fact that it only generates a single output, a neural network that consists of a single layer is known to as a perceptron.

Evaluation Metrics: The outcome of a classification problem can be either accurate or incorrect, and all of the potential outcomes can be broken down into one of these four conditions:

- **True Positive (TP):** actual malicious attacks are correctly identified as attacks;
- **True Negative (TN):** actual normal records are correctly identified as normal;
- **False Positive (FP):** actual normal records are falsely identified as attacks which is also known as false alarms.
- **False Negative (FN):** actual malicious attacks are falsely identified as normal records.

On this basis of TP, FP, TN, FN, various performance measurements namely, accuracy, detection rate, false positive rate, precision and F-measure score can be defined as follows.

- **Accuracy:** It is the amount of records with accurate categorizations expressed as a percentage of the total number of records.
- **Precision:** It is the amount of actual attacks expressed as a percentage of the total number of incidents that were recorded as attacks.
- **Detection rate (DR):** It is the amount of occurrences that are categorised as attacks as a percentage of the total number of attacks.
- **False positive rate (FPR):** It is the total number of records that can be categorised as attacks as a percentage of the total number of normal records.
- **F-measure score:** It is a thorough analysis that takes into account both the accuracy and the detection rate. It is calculated using the harmonic mean of their values. If the F-measure is higher, then the precision and DR will also be higher.

On the one hand, when seen from the perspective of a classifier, precision and detection rate are indeed a pair of measures that are in direct opposition to one another. A better precision results in a lower number of false positives, whereas an increased detection rate results in a lower number of false negatives. For instance, the detection rate will improve, but the precision will fall, and conversely if more suspected assaults are categorised as actual attacks (the worst-case scenario is that all data are categorized as actual attacks). Therefore, there is no use in concentrating on a specific high precision or DR. A distinct DR is also an important indicator that should be taken into consideration in addition to a separate detection rate. In contrast hand, from the perspective of intrusion detection, the tolerance for intrusion is quite low, particularly in some severe contexts.

4. Result and Discussion

The purpose of the two experiments is to investigate the effectiveness of an RNN-LSTM-based IDS framework for binary and 5-group classification, respectively. When using binary classification, data is categorised as either normal or anomalous, however when using 5 group classification, data is categorized as normal, DOS, R2L, L2R, and probe. Experiments of varying types were carried out so that the results could be compared to those of other machine learning strategies. As can be seen in tables 1 and 2, the effectiveness of a number of other machine learning classifiers was evaluated and contrasted with that of RNN-LSTM for both classifications. Consider the following table 1, which depicts the performance of 5 conventional classifier with proposed RNN-LSTM method based on binary classification.

Table 1: The performance of 6 conventional machine learning classifier with RNN-LSTM based on binary classification

	SVM	NB	DT	ANN	RF	RNN-LSTM
KDD Cup99	82.03%	69.54%	76.58%	81.06%	77.42%	83.29%
NSLKDD	66.18%	42.31%	55.79%	63.99%	57.36%	68.59%

From the above table 1, it is observed that performance of RNN-LSTM classifier based on binary classification method is 83.29% and 68.59% using KDD Cup 99 and NSLKDD dataset which is better as compared to other conventional machine learning classifier.

Consider the following table 2, which depicts the performance of 5 conventional classifier with proposed RNN-LSTM method based on 5-group classification.

Table 2: The performance of 6 conventional machine learning classifier with RNN-LSTM based on 5 group classification

	SVM	NB	DT	ANN	RF	RNN-LSTM
KDD Cup99	78.12%	72.82%	74.43%	75.42%	74.61%	81.30%
NSLKDD	58.41%	49.72%	55.79%	55.41%	51.91%	64.68%

From the above table 2, it is observed that performance of RNN-LSTM classifier based on 5 group classification method is 81.30% and 64.68% using KDD Cup 99 and NSLKDD dataset which is better as compared to other conventional machine learning classifier.

.

Following figure 2, depicts the performance of 5 conventional machine learning classifier with RNN-LSTM based on binary classification

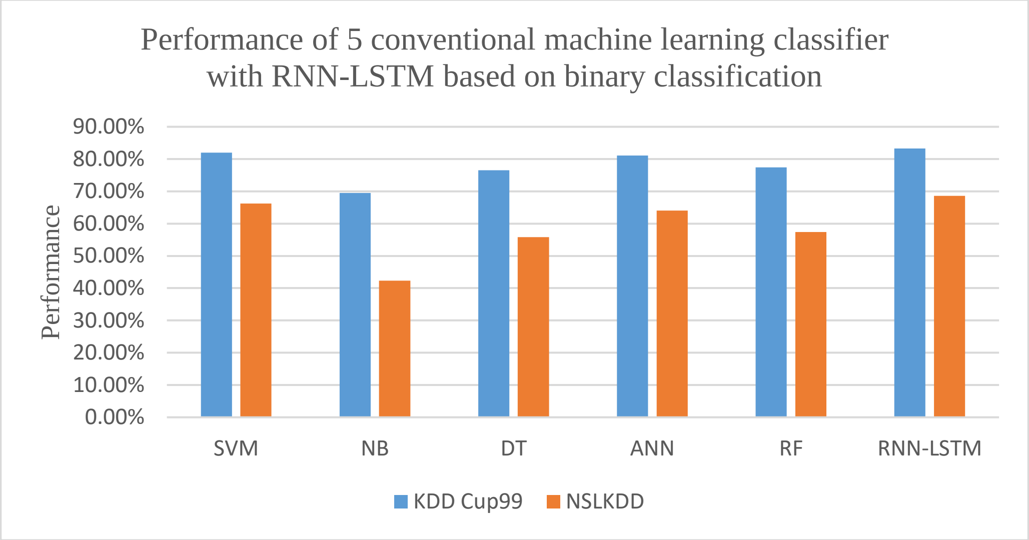


Fig. 2: The performance of 6 conventional machine learning classification methods with RNN-LSTM method based on binary classification

Following figure 3, depicts the performance of 5 conventional machine learning classification models with RNN-LSTM method based on 5-group classification.

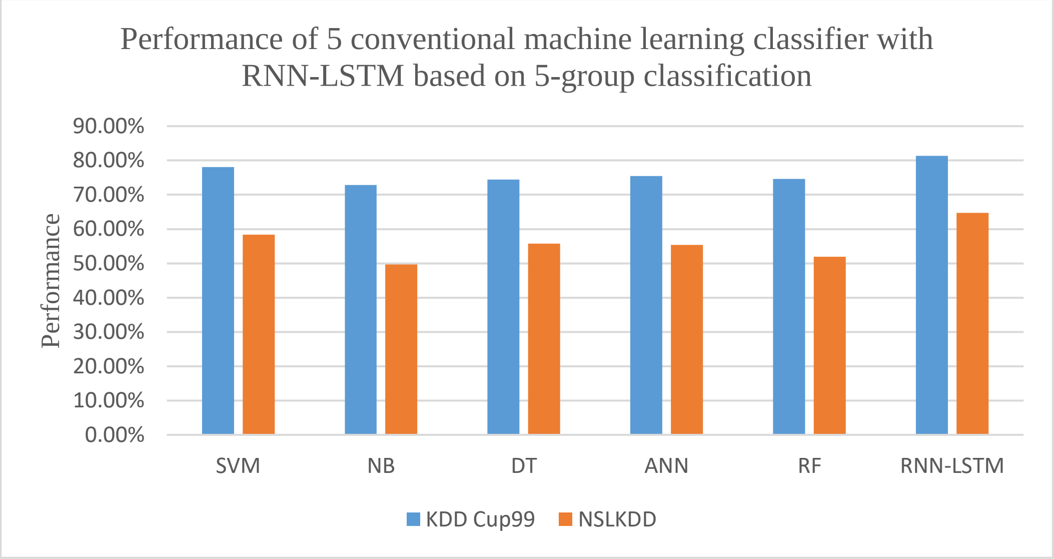


Figure 3: The performance of 5 conventional machine learning classification methods with RNN-LSTM method based on 5-group classification

Thus, it is observed from the two experiments that the performance of RNN-LSTM method based on binary classification is 83.29% and 68.59% using KDD Cup 99 and NSLKDD dataset which is better as compared to other conventional machine learning classifier and 5-group classification method.

5. Conclusion and Future work

In this research, a hybrid intrusion detection system, RNN-LSTM framework is proposed using standard benchmarked datasets namely KDDCup99 and NSLKDD. Two experiments namely binary classification and 5-group classification is performed. Using these experiments, the performance of conventional machine learning techniques is compared with proposed RNN-LSTM method using KDDCup99 and NSLKDD dataset. It is observed from these two experiments that the performance of RNN-LSTM method based on binary classification is 83.29% and 68.59% using KDD Cup 99 and NSLKDD dataset which is better as compared to other conventional machine learning classifier and 5-group classification method. The suggested architecture is capable of achieving superior performance in both Host based IDS and Network based IDS in comparison to conventional machine learning classification methods that have been previously deployed. The proposed framework has the capability to gather activity on both the network level and the host level in a decentralized way. This makes it possible to detect attacks with more precision. The system that is being suggested in this research is primarily dependent on theoretical validation. In order to prove its practical use, a significant amount of engineering work needs to be done. The next step might be to improve the system in order for it to be used in actual network configurations and be put into action in a way that is more time and cost effective.

References

[1] H. Yang, Y. Bai, T. Chen, Y. Shi, R. Yang and H. Ma, "Intrusion Detection Model For Power Information Network Based On Multi-layer Attention Mechanism," 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 2022, pp. 825-828, doi: 10.1109/ITAIC54216.2022.9836897.

[2] S. Amutha, K. R, S. R and K. M, "Secure network intrusion detection system using NID-RNN based Deep Learning," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-5, doi: 10.1109/ACCAI53970.2022.9752526.

[3] K. Yu, K. Nguyen and Y. Park, "Flexible and Robust Real-Time Intrusion Detection Systems to Network Dynamics," in IEEE Access, vol. 10, pp. 98959-98969, 2022, doi: 10.1109/ACCESS.2022.3199375.

[4] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," in IEEE Access, vol. 10, pp. 99837-99849, 2022, doi: 10.1109/ACCESS.2022.3206425.

[5] V. Rajasekar, S. Sarika, V. S, I. T. Joseph S and K. K. S, "An Efficient Intrusion Detection Model Based on Recurrent Neural Network," 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, 2022, pp. 1-6, doi: 10.1109/ICDCECE53908.2022.9793016.

[6] U. Mbasuva and G. -A. L. Zodi, "Designing Ensemble Deep Learning Intrusion Detection System for DDoS attacks in Software Defined Networks," 2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM), Seoul, Korea, Republic of, 2022, pp. 1-8, doi: 10.1109/IMCOM53663.2022.9721785.

[7] I. Ullah and Q. H. Mahmoud, "Design and Development of RNN Anomaly Detection Model for IoT Networks," in IEEE Access, vol. 10, pp. 62722-62750, 2022, doi: 10.1109/ACCESS.2022.3176317.

[8] A. Singh, V. Bhandari and R. Srivastava, "Optimization Accuracy of Intrusion Detection of Imbalanced Network using PCA and Conv1D-LSTM Technique," 2022 3rd International Conference for Emerging Technology (INCET), Belgaum, India, 2022, pp. 1-6, doi: 10.1109/INCET54531.2022.9824763.

[9] B. Budler and R. Ajoodha, "Comparative Analysis of Deep Learning Models for Network Intrusion Detection Systems," 2022 IEEE 2nd Conference on Information Technology and Data Science (CITDS), Debrecen, Hungary, 2022, pp. 45-50, doi: 10.1109/CITDS54976.2022.9914128.

[10] H. Babbar, O. Bouachir, S. Rani and M. Aloqaily, "Evaluation of Deep Learning Models in ITS Software-Defined Intrusion Detection Systems," NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2022, pp. 1-6, doi: 10.1109/NOMS54207.2022.9789829.

[11] R. Kavitha and S. Amutha, "Performance Analysis of Deep Neural Network and LSTM models for Secure Network Intrusion Detection System," 2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), Goa, India, 2022, pp. 390-396, doi: 10.1109/ICCCMLA56841.2022.9989253.

[12] D. Ding, L. Zhu, J. Xie and J. Lin, "In-Vehicle Network Intrusion Detection System Based on Bi-LSTM," 2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 2022, pp. 580-583, doi: 10.1109/ICSP54964.2022.9778620.

[13] G. Ketepalli and P. Bulla, "Feature Extraction using LSTM Autoencoder in Network Intrusion Detection System," 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2022, pp. 744-749, doi: 10.1109/ICCES54183.2022.9835788.

[14] B. Deore and S. Bhosale, "Hybrid Optimization Enabled Robust CNN-LSTM Technique for Network Intrusion Detection," in IEEE Access, vol. 10, pp. 65611-65622, 2022, doi: 10.1109/ACCESS.2022.3183213.

[15] Y. Yu, X. Zeng, X. Xue and J. Ma, "LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 12, pp. 23906-23918, Dec. 2022, doi: 10.1109/TITS.2022.3190432.

[16] J. Li, "Research on Intrusion Detect System of Internet of Things based on Deep Learning," 2022 International Conference on Machine Learning and Knowledge Engineering (MLKE), Guilin, China, 2022, pp. 55-58, doi: 10.1109/MLKE55170.2022.00016.

[17] M. D. Rokade and S. S. Khatal, "Detection of Malicious Activities and Connections for Network Security using Deep Learning," 2022 IEEE Pune Section International Conference (PuneCon), Pune, India, 2022, pp. 1-6, doi: 10.1109/PuneCon55413.2022.10014736.

[18] J. Bi, Z. Guan and H. Yuan, "Hybrid Network Intrusion Detection with Stacked Sparse Contractive Autoencoders and Attention-based Bidirectional LSTM," 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Prague, Czech Republic, 2022, pp. 6-11, doi: 10.1109/SMC53654.2022.9945600.

[19] A. Bhardwaj, S. S. Chandok, A. Bagnawar, S. Mishra and D. Uplaonkar, "Detection of Cyber Attacks: XSS, SQLI, Phishing Attacks and Detecting Intrusion Using Machine Learning Algorithms," 2022 IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT), New Delhi, India, 2022, pp. 1-6, doi: 10.1109/GlobConPT57482.2022.9938367.

[20] M. A. Razib, D. Javeed, M. T. Khan, R. Alkanhel and M. S. A. Muthanna, "Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework," in IEEE Access, vol. 10, pp. 53015-53026, 2022, doi: 10.1109/ACCESS.2022.3172304.

[21] M. Asaduzzaman and M. M. Rahman, "An Adversarial Approach for Intrusion Detection Using Hybrid Deep Learning Model," 2022 International Conference on Information Technology Research and Innovation (ICITRI), Jakarta, Indonesia, 2022, pp. 18-23, doi: 10.1109/ICITRI56423.2022.9970221.

[22] A. F. Almutairi and A. Abdulghani Alshargabi, "Using Deep Learning Technique to Protect Internet Network from Intrusion in IoT Environment," 2022 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA), Ibb, Yemen, 2022, pp. 1-6, doi: 10.1109/eSmarTA56775.2022.9935467.

[23] H. Chi and C. Lin, "Industrial Intrusion Detection System Based on CNN-Attention -BILSTM Network," 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS), Huaihua City, China, 2022, pp. 32-39, doi: 10.1109/ICBCTIS55569.2022.00019.

[24] Z. Jie, "IoT-Network Attack Detection with Optimized Recurrent Neural Network and Optimal Feature Selection," 2022 IEEE 2nd International Conference on Data Science and Computer Application (ICDSCA), Dalian, China, 2022, pp. 951-957, doi: 10.1109/ICDSCA56264.2022.9987890.

[25] H. Hou, Z. Di, M. Zhang and D. Yuan, "An Intrusion Detection Method for Cyber Monintoring Using Attention based Hierarchical LSTM," 2022 IEEE 8th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Jinan, China, 2022, pp. 125-130, doi: 10.1109/BigDataSecurityHPSCIDS54978.2022.00032.