Enhancing Network Security with Deep Learning-Based Intrusion Detection Systems

Shrikant Telang[1], Rekha Ranawat[2]

[1]Computer Science Enginnering, SAGE University, Indore, India, Email: schshrikanttelang@gmail.com
[2]Computer Science & Engineering, SAGE University, Indore, India, Email: rekharathore23@gmail.com

Received: 15.07.2024 Revised: 13.08.2024 Accepted: 10.09.2024

ABSTRACT
Due to the vast quantity of services that are provided to users online and the immense amount of digital private information that has been transferred in recent years, the majority of individuals now rely heavily on the internet in their everyday lives. On the other hand, as internet usage increases, so does the assault surface for cyberattacks. The internet will be considerably more susceptible if no effective defense mechanism is put in place, which will increase the likelihood that data will be compromised or leaked. This highlights the significance of deep learning approaches for intrusion detection systems (IDS) and how crucial IDS are to network security. Sophisticated attacks are typically difficult to detect for traditional IDS methods, which results in more false positives and undetected threats. To overcome these limitations, this work proposed an empirical detection system of different deep learning models i.e., Long-Short Term Memory (LSTM),Multi-layer Perceptron(MLP), Linear Support Vector Machine(SVM), Quadratic Discriminant Analysis, in these models, the LSTM model does best with an accuracy of 96 %, precision of 92%, recall score at 93%, and F-1 smart value as well get up to level with most traditional methods. Compared with traditional machine learning algorithms, deep-learning models are advantageous for IDSs to model complex and sequential data sets with results which showsthe improved detection rates while reducing false alarms and concluded that deep learning-based IDS can offer more steady and dependable security solution in unpredictable network environments.

Keywords: Deep Learning, Intrusion Detection System (IDS), Network Security, Long Short-Term Memory (LSTM), Anomaly Detection.

1. INTRODUCTION

The internet networked like never before, security of networks has become extremely important in these times when almost everyone is vulnerable to cyber threats. Data breaches and other threats have been thwarted by a security solution known as Intrusion for years, networks have been monitored by detection systems (IDS) to identify malicious activity or illegal access. Cyberattacks are becoming more advanced day by day and it has become imperative to predict highly developed IDS solutions that can detect these threats with high accuracy rate & low false positive count. Traditional IDS approaches, which are rule-based and use mostly known signatures for detection often fall short to detect new unknown threats or very subtle deviations in traffic. This suggests that more sophisticated techniques, such as deep learning approaches for IDS need to be incorporated in order to mitigate these limitations.

Deep Learning

Within the broader subject of artificial intelligence (AI) and machine learning, deep learning is a subset. In domains like natural language processing, picture identification, and predictive analytics, this approach performs remarkably well. The fact that a neural network can be trained to represent highly complex patterns and relationships in data also makes it very appropriate for creating models where high level of accuracy is needed or when the association between inputs-output pairs changes over time. The use of deep learning techniques in IDS opens up the possibility to enhance intrusion detection largely because these types of systems can learn from abundant data and adapt over new varieties of attacks without any necessity for explicit programming or a clear precedence set.

IDS has evolved from traditional techniques like signature-based and anomaly based approaches to more advanced methods with ML incorporated into this. Signature-based detection, which checks each file packet against a database of known attack patterns and is perfect for recognizing known threats but fails to identify new or changed attacks. By contrast, anomaly-based detection notices when things are different from a standard process in place and is hence good at picking up novel attacks. Unfortunately, it is also generally subject to a high percentage of false positives because normal deviations in network behaviors tend to get classified as intrusion. To overcome these challenges, researchers and practitioners have been investigating machine learning on leading to deep learning techniques as complementary ways to augment the capabilities of IDS.

Many of the machine learning techniques were employed for dealing with IDS, like Support Vector Machines (SVM), Decision Trees and Random Forest. Because these methods can be trained on data and recognize the appearance of a certain type malicious activity, they are considerably more versatile than traditional signature based systems. They can however be very limited when it comes to dealing with large-scale, high-dimensional data and may not always capture complex temporal dependencies in network traffic. This is where deep learning methods, in particular for sequence data such as Long Short-Term Memory (LSTM) networks, enters into.Recurrent Artificial neural networks, of which Neural Networks (RNNs) are a specific instance, establish directed cycles between nodes through their connections, which captures that temporal information within the sequence for instance in time-related problems. Sound techniques are hitting broad interest in the popular exercises, as an example, language (spoken) model office and time sequence predictions LSTM networks can be used to analyze sequences of network traffic in the context of Intrusion Detection Systems, looking for time-based patterns which could reveal an ongoing attack. LSTM networks can notice small anomalies that vary according to the context, which are undetectable by other methods through learning from historical data so they help us detect known and unknown risks as well.

This paper is using the deep learning techniques, with an extra emphasis on LSTM networks to improve IDS. Therefore, the goal so far is to investigate how well these advanced methodologies could solve existing problems regarding effectiveness and precision that traditional IDS approaches have then they fail to reduce its false positives. To this end, we create and compare multiple models like Linear Support Vector Machine (SVM), Quadratic Discriminant Analysis, Multi-Layer Perceptron(MLP) and LSTM to find out about how much effectively these models are in detecting intrusions.Our study shows that LSTM networks are robust outperformer with respect to all measures. The LSTM model on the other hand shows accuracy 96%, precision 92%, recall 93% and F1-score90%. These results are significantly better than the others, with an accuracy of 92% and slightly worse scores on other metrics for Multi-Layer Perceptron (MLP) which is in second place. LSTM networks can capture the complex temporal patterns in network traffic that are common with malicious behavior, hence they provide better results.

LSTM networks are resilient to learning mistakes LSTMs is the only kind of network that learn error exactly. The LSTM model is also the best of all models in both metrics: having lower MAE, MSE and RMSE than every other. The R-squared (R2) 0.85 for LSTM model shows that our predictions vs actual data is predicted well and it further intensifies the IoT-IoT invasion detection capability of Our Approach

LSTM networks in IDS — other than performance metrics This method beats this in various ways that are common. One such significant advantages they have, is that their capacity to grow over time with fresh diverse kinds of strikes. While tradition IDS only depend on the signatures hence making them outdated frequently and needs new threat pattern to be updated, LSTM networks can update them-self through time. Which is all the more crucial in our rapidly changing cyber landscape of constantly emerging attack vectors and methodologies.

The use of deep learning on IDS can provide a means to create more efficient and speedier systems. Any time the data is increases with network traffic volumes grow then traditional IDS methods may fall. Sort to handle. It was designed to handle large datasets and analyze patterns of behavior in real time, making it flexible enough for today's networks. The new way for a PI to learn is very promising, combining the scalability feature which elucidating down in this section making difficult-learning oriented-networks from one network and it LZH; their efficiency with LSTM networks.

A major dimension for network security is intrusion detection systems (IDS) and amongst any other example in this area, deep learning methods particularly LSTM networks are probably the best one. Though it has some limitations but then also we can to settle on that deep learning based IDS itself more reliable because of problems solved in traditional ways, and IDC make sure better service than precision / recall & adaptable for range of cyber threats. As deep learning is going to be an upcoming methodology for IDS that can even give the best results in detection accuracy and has trustable features against incoming cyberattacks. This paper intends to contribute toward this endeavor by investigating the potential of deep learning models for IDSs and illustrates how these bleeding-edge methods have a transformative effect on network security.

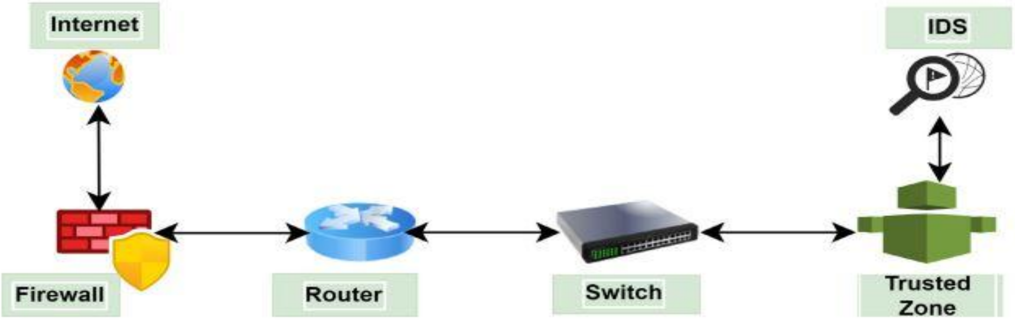


Figure 1. Passive implementation of NIDS.

the introduction may highlight possible aims of this review: to conduct an extensive survey about the different ML methods and DL techniques used in IDSs; establish how these tools have performed when it comes to identifying incidents; discuss problems with existing work [challenges/limitations]; or navigate upcoming trends for further development on related issues. This promises a deep look at the cutting-edge AI technologies and what this means for cybersecurity.

2. BACKGROUND STUDY

The concept of Intrusion Detection System (IDS) has been introduced with the development in networking and internet world. The basic concept of IDS is to take some data from network or system device and try put some logic on this data if there are any malicious activity happening in the size and alert admin. When intrusion detection was developed early at the beginning, efforts were directed toward simple misuse and anomaly patterns. IDS technologies evolved with the increase in volume, complexity of cyber threatsCDATA Now a day they use wide range of techniques like signature-based detection, anomaly-based or behavior based detections (outlier analysis find deviation from normal behavior,stateful protocol Analysis it can look for patterns that would be hard to identify with fixed rules), pattern matching. In addition, the greater usage of advanced technologies like machine learning and artificial intelligence has further triggered a revolutionized version of IDS that can more dynamically respond to emerging threats. Even as their technology has improved, IDS still have issues like high false positive rates and a requirement for rolling out new detection mechanisms to counter the ever increasing cyber threats. Continuous development of IDS is an important part in general cybersecurity activities to defend digital assets, which are becoming more and tighter coupled.

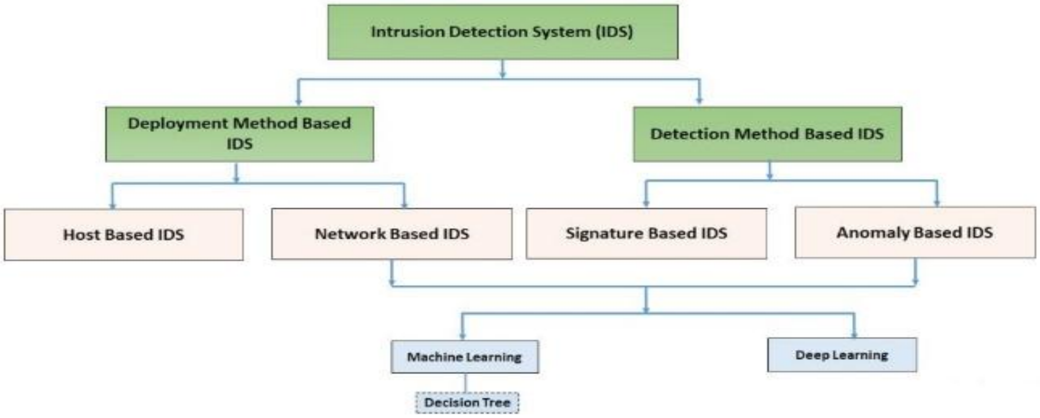


Figure 2. Taxonomy for classifying intrusion detection systems.

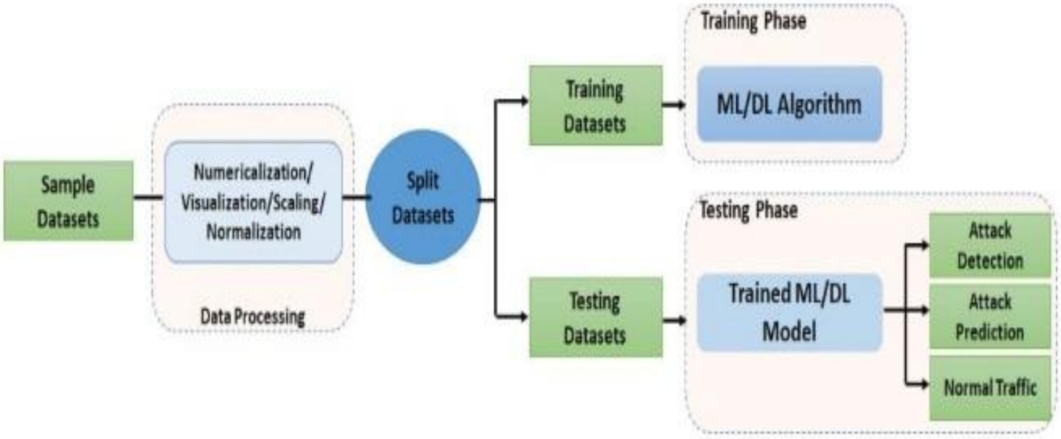


Figure 3. A network intrusion detection system methodology is proposed, using generic machine learning and deep learning approaches.

3. LITERATURE REVIEW

The importance of Software Defined Networking (SDN) on the internet infrastructure to deliver semantic networking beneficially oversimplifies network management for full blown companies and complete economies making life a bed of roses during service interruptions or online scams. Software-Defined Networking (SDN) has been a popular research field as a means of addressing these risks by fusing powerful machine learning algorithms with intrusion detection systems.Intriguing Labors -Artificial neural networks, of which Neural Networks (RNNs) are a specific instance, establish directed cycles between nodes through their connections. The goal was to create a 2-phase hybrid feature selection approach that combines the correlation based and medium approaches. For the NSL-KDD dataset [1], LGiBTS works best combined with LightGBM for tag attacks Identification/Classificationattacks Prediction. The Internet and its security have grown a lot in recent times. The advent of the IoT has also been a major reason behind all fraudulent traffic. Moreover, the implementation of machine learning (ML) requires advanced intrusion detection systems IDSs. We assess the impact of VGG-16, DenseNet based transfer learning models and image filters on feature extraction in a machine-learning-based IoT IDS. One of them combined a Random forest and support vector machines (SVM) on the IEEE data port dataset, alongside with VGG-16 that achieved high accuracy after stacking [2].

There is a greater risk in the cyber-space due to increasing number of IoT devices. Conventional Intrusion Detection System (IDS) solutions are inadequate in Software-Defined Networking (SDN)-based environments for integrating both conventional and Internet of Things IoT protocols. This paper proposed an Intrusion Detection System (IDS) in IoT network which uses Long Short-Term Memory (LSTM) and Software-Defined Networking(SDN). Even with OT the relative computer performance is necessary to retain timing and detection capabilities. Performance test on SDNIoT (Software-Defined Networking for the Internet of Things) Benchmark from ASoC Datasets Finally, the performance of ML/deep learning model was verified in a two datasets specifically created for IOD related procedures. The results of the test show a high degree classification accuracy for attack types (ATC) [3]. Increased network data from the technological advancements has increased its security risk. In this paper, we introduce an Intrusion Detection System (IDS) framework where it uses Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU) Based Recurring Neural Networks with various Machine Learning algorithms. Feature selection with XGBoost on the NSL-KDD and UNSW-NB15 The best combination is achieved by XGBoost-LSTM[4]. During the digital revolution, it is unavoidable that some data sent over a network without passing through any security checks must stay private. Network Intrusion Detection Systems are the solution for that. This work aims towards the design of datasets for training and testing such a system. In this investigation, the CIDDS-001 dataset is examined using machine learning methods to predict only DDoS attacks with performance measurements [5]. In the information age, cybersecurity is of vital concern. IDSs face a greater number of new threats thanks to the always evolving settings that ICT systems experience, which in practice makes it difficult not only to detect but also classify all unusual and harmful activities. More specifically, in [6], the authors of this study have investigated many adversarial machine learning (AML) attacks against Intrusion Detection Systems (IDSs), and their countermeasures.

Industrial Automation and Industrial control systems often deal with critical infrastructure (CI) of a nation. This work provides an in-depth exploration of public datasets available for training ML models from the security domain. It also investigates the recent works on applying machine learning approaches to protect critical infrastructures by advanced intrusion detection systems [7]. Cybersecurity is critical as we get more and more of these IoT devices. To be more specific, this work proposes a CNN-GRU model for recognizing attacks in an Intrusion Detection System (IDS). The method is developed on a CICIDS-2017 benchmark dataset. Result: The accuracy levels have bettered many previous approaches to detection and comparison [8]. In this survey paper, various machine learning (ML) and deep learning (DL) based intelligent techniques are utilized alongside the advancements in Intrusion Detection Systems (IDSs), particularly for Network Intrusion Detection Systems(NIDS); hence compiling an integrated methodology. This article talks about the proposed work on that attacked dataset and how it is not enough to be specific. In scenario IV, an in-depth overview of the methodology and evaluation metric are adopted to describe along with network security problems connected through prominent datasets mentioned before using a significant 1% subset randomly chosen from both those dataset networks discussed in Section III. References Detection strategy based on the decision trees has been well addressed by rearner [9]. To that, the IoT surge has provided a huge upsurge in number of cyberattacks. The improved IoT Intrusion Detection System (IDS) uses a deep Fully Connected (FC) network model. Hence it could be said that iDop can help in securing IoT networks [10].

Interconnection of Things (IoT): It is a collection of intelligent gadgets that communicate and share information online. Furthermore, other sectors such as healthcare, Intelligent transportation systems and smart cities are able to exploit the benefits of this platform due to advances in Internet Things (IoT). It requires that you can prioritize IoT security and do it correctly. What is IDSIDS full form = Intrusion Detection System. They do this by monitoring traffic on the internet using systems that look for infiltration attempts and stop them within seconds or minutes. This research will compare the quality-of-service metrics with the current security methods implemented in IoT network security. Modern deep learning techniques were used to create the incredibly effective Intrusion Detection System (IDS) and classification platform known as Fuzzy CNN. It also is very effective method for detection of DOS attacks and reduce false positives [11].

With the everyday operations moving digitally there is an increase in network vulnerabilities. Just as detecting viruses on your computer is based on virus signatures, network intrusion detection depends entirely in its majority of shortcomings (namely there are many new vulnerabilities actually) from known and very old patterns. In this work, we put forth a novel NIDS with DL model which is trained on real time traffic using CICID2018 and Edge_IIoT datasets. NIDS has a good efficacy for classifying numerous kinds of network intrusions [12]. UTMIDSs recognize more advanced threats than signature-based solutions can alone. Our work provides a novel ensemble-based machine learning method for intrusion detection which is evaluated on multiple publicly available datasets. Overall, the random forest model developing is better than fixed features by only three feature selection methods of correlation, mutual information and principal component analysis. Moreover, all three methods which were selected in conjunction with filter outperform Random Forest even considering FPR. Ensuring the security of block chain and Internet of Things (IoT) systems: As traditional issues like data integrity, denial-of-service (DoS), etc. are a major issue in securing IoT networks running on block tech solutions. In another work, AI is applied to recognize people who threaten our society using a system model. In turn, it serves as an aid to improve data security through block chain technology. They tried to send the IoT data using Deep Learning algorithms and classified smart contracts into secure or not in an end-to-end security pipeline [14]. Growth in the number of cyberattacks focused on big businesses over time requires a responsible attitude towards cybersecurity requirements. To detect and classify unauthorized access attempts, we use machine learning algorithms. Madhuri Soni and Ravi Gupta present two cyberattack detection methods based on machine learning with the NSL-KDD dataset [15].

Basically, networks become more prone to cyber-attacks when automation is being applied in them. This chapter is intended to further implement feature selection in a mixed way, that we will use the Pearson correlation coefficient with some other machine learning model actually RF. Therefore, the goal is to catch intrusions with high accuracy. The dataset utilised was TON_IoT [16]. Performance wise Decision trees and multilayer perceptron (MLP) models are better than other machine learning (ML), Deep Learning(DL) models. The rise in cyber threats calls for security beyond basic antivirus software and firewalls. Study [17] evaluate attacks in the UNSW-NB15 and NSL-KDD dataset through machine-learning & deep-learning methods. Dispute-tie techniques are used by the researchers in order to obtain accurate classification results and improve detection rate of intrusion detection systems. The ubiquity of these technologies has given rise... Then we train and compare several deep neural network models, such as convolutional #1584502400# networks (CNNs) for image data [13] and long short-term memory(LSTM), with the CIC-IDS 2017 dataset of intrusion detection ([18]). When it comes to a Distributed Denial of Service (DDoS) attack, the detection system needs to be absolutely accurate. In this work, we have proposed a CNN-LSTM Deep learning model that has been able to produce better results than baseline methods on the NSL-KDD dataset [19]. The network, especially against Denial of Service (DoS) attacks. Today we will see how to create a Wireless Intrusion Detection System (WIDS) with the tools provided in Kali Linux. An experiment of multiple WAN networks has proven the effectiveness in threat detection and mitigation capabilities [20]. The pandemic is pushing the way suppliers and consumers interact toward online platforms. Therefore, the demand for more responsible and secure solutions is increasing. The purpose of this project is to use a Naive Bayes algorithm in order to create an intrusion detection system that will monitor the activity on type web server Apache. On the IEEE data set [21], AMOS-ANN achieves this accuracy using cross-validation approach.

4. PROPOSED METHODOLOGY

4.1 Proposed Flowchart

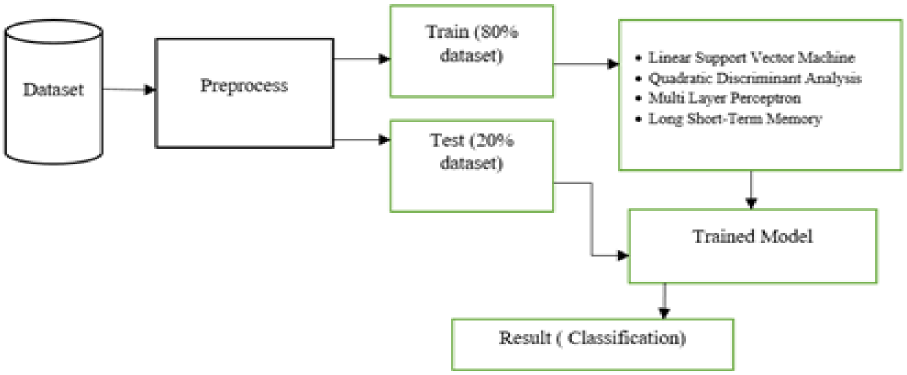


Figure 4. Proposed Flowchart

The diagram 4 illustrates a procedure for machine learning categorization. The procedure begins with a dataset that undergoes preprocessing to prepare it for both training and testing. Next, the dataset is partitioned, allocating 20% of the data for the training set and 80% for the testing set. We use many machine learning models, including Linear Support Vector Machine, Quadratic Discriminant Analysis, Multi-Layer Perceptron, and Long Short-Term Memory. These models are trained on an 80% portion of the dataset specifically designated for training purposes. After obtaining the trained models, they analyze each test data to determine its classification and then assess the accuracy of the labels assigned by our trained model.

4.2 Algorithm: Intrusion Detection System (IDS)

Step 1: Data Collection

- **Input:** Network traffic data, system logs, or other relevant datasets.
- **Output:** Collected dataset for analysis.
- Gather information from a variety of sources, including system events, logs, and network traffic.

Step 2: Data Preprocessing

- **Input:** Raw collected data.
- **Output:** Preprocessed dataset ready for training and testing.
- **Data Cleaning:** Remove any noise, irrelevant data, and fill in missing values.
- **Feature Selection/Extraction:** Identify and select important features that contribute to detecting intrusions.
- **Data Normalization/Scaling:** Normalize or scale data to ensure consistency across all features.
- **Label Encoding:** If necessary, encode categorical labels into numerical format.

Step 3: Data Splitting

- **Input:** Preprocessed dataset.

- **Output:** Training dataset (80%) and Testing dataset (20%).
- Using an 80-20 split ratio, divide the preprocessed data into training and testing datasets.

Step 4: Model Selection and Training

- **Input:** Training dataset.
- **Output:** Trained models.
- Select multiple machine learning algorithms such as:
  - Linear Support Vector Machine (SVM)
  - Quadratic Discriminant Analysis (QDA)
  - Multi-Layer Perceptron (MLP)
  - Long Short-Term Memory (LSTM)
- Train each selected model on the training dataset.

Step 5: Model Testing

- **Input:** Testing dataset and trained models.
- **Output:** Prediction results from each model.
- Evaluate each trained model using the testing dataset.
- Generate prediction results for each model.

Step 6: Model Evaluation

- **Input:** Prediction results and actual labels from the testing dataset.
- **Output:** Performance metrics for each model.
- Metrics like F1-score, accuracy, precision, and recall may be used to compare the true and predicted labels.
- Identify the model with the best performance based on these metrics.

Step 7: Intrusion Detection

- **Input:** New, incoming data.
- **Output:** Classification of data as normal or intrusion.

5. IMPLEMENTATION AND RESULT

5.1 Dataset

Most commonly data set of IDS and network security benchmark, used by infringer the NSL-KDD It has the same number of columns but contains 551+ records where old data also contain just 489. This dataset was used to evaluate intrusion detection systems (IDS) served as a tool for the recognition of computer network assaults. KDD Cup is an annual competition since 1999. Known problems with the KDD Cup 1999 dataset include an artificial distribution of attack types and a limited variation in assault scenarios.
Link: [21]

5.2 Experimental Analysis

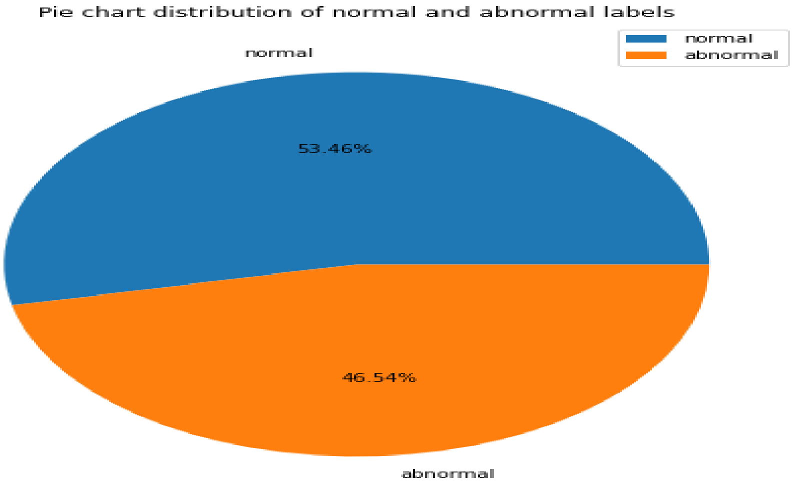


Figure 5. Binary classification

The figure 5 shows the distribution of normal/abnormal labels in dataset. In the chart you can see that 53.46% of data have "Normal" and 46.54% has abnormal case so labels are not well balanced in this dataset which we know as imbalanced classes but ideally binary class should be balanced if its near to equal then great however need little extra care whenever they are off target else it will towards underperforming your model on most occasions trolls back). It tells us that the three tends to be more normal instances than abnormal cases a fairly balanced dataset

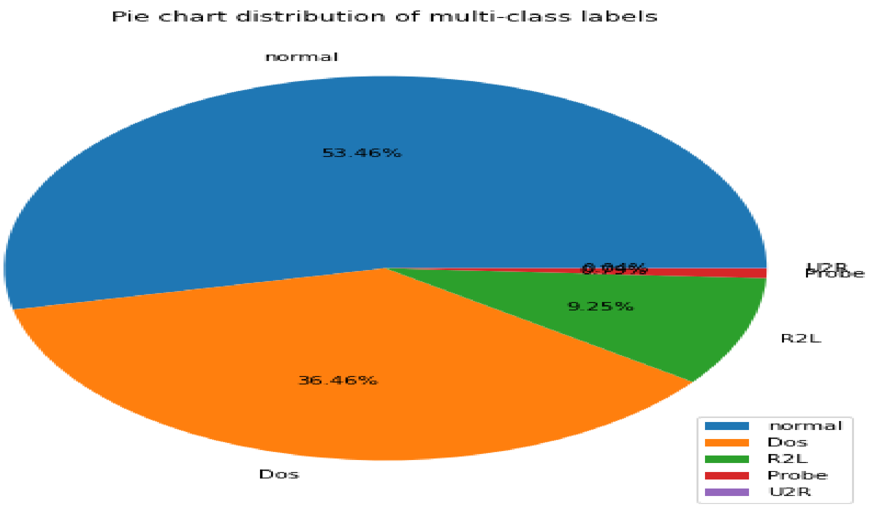


Figure 6. Multi class classification

The figure 6 represents the percentage of several types associated with categories that illustrate multi-class labels in a dataset, which goes beyond just showing you how network traffic e.g., or behaviors split up. Most data, 53.46%, is normal 36.46% of the dataset represent “Dos” (Denial of Service) attacks R2L (Remote to Local) attacks weigh in at 9.25% and Probe are only a tiny number on 0.9%. Only 0.02% belong to the category "U2R" (User to Root). This chart illustrates the dataset contains mainly of normal and Dos attack, while other attacks are in lesser percentages.

4.3 Long Short-Term Memory (LSTM)

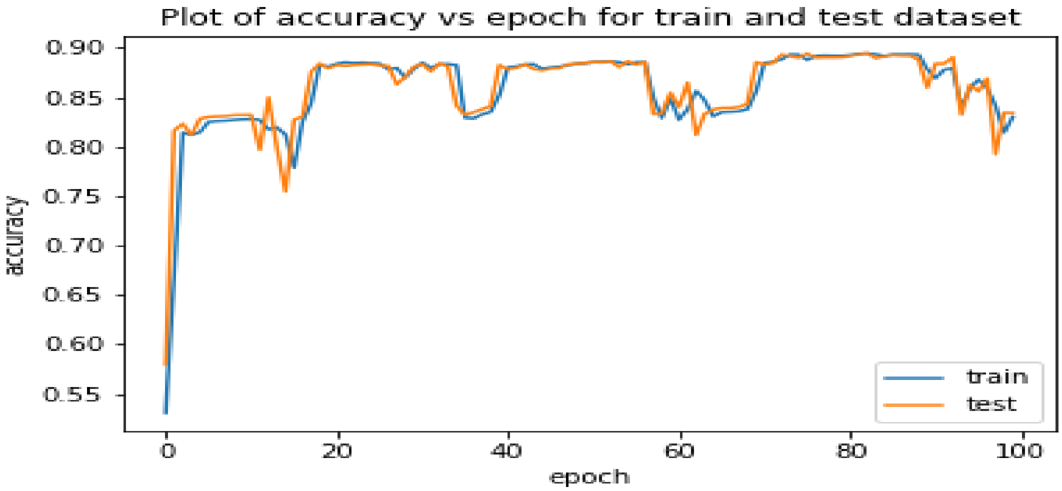


Figure 7. Accuracy of test and training data throughout 100 epochs.

The figure 7 Showing the Accuracy of both training and test data over 100 epochs (model generation time) From the beginning, training and nb epochs testing accuracies are very low, respectively. (noticeable oscillations during first 20 epochs) Note that as training goes on the accuracies become stable and tend to converge following a similar pattern, but well above 80% accuracy for both datasets. Our model does not exhibit significant overfitting or under fitting, as seen by the near alignment of the training and testing accuracy curves. Ultimately the model has a very high accuracy since few epochs, and we can bet it learns a base pattern to get good performance.

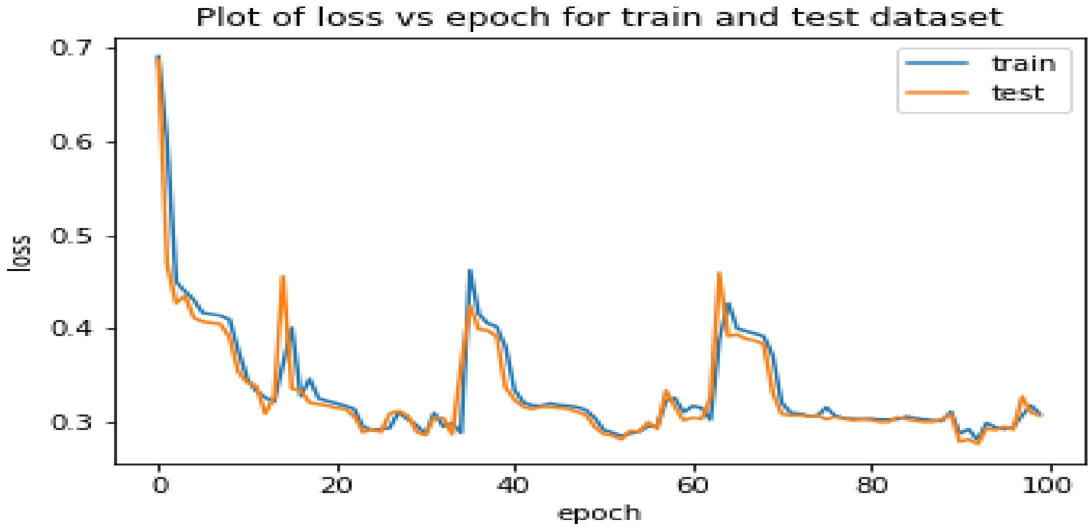


Figure 8. The loss across 100 epochs for the training and testing datasets.

The figure 8 depicts the loss for both the training and testing datasets over 100 epochs during model training. Initially, the loss is relatively high, around 0.7, but it rapidly decreases within the first few epochs. Throughout the training process, there are a few noticeable spikes in loss at various points, particularly around epochs 20, 40, and 60. Despite these fluctuations, the overall trend shows a steady decline in loss for both datasets, stabilizing around 0.3 as training progresses. The similar pattern in both the training and testing loss curves indicates that the model is learning effectively without significant overfitting, as the loss values converge closely. The final low loss values suggest that the model is performing well in minimizing error on both the training and testing datasets.

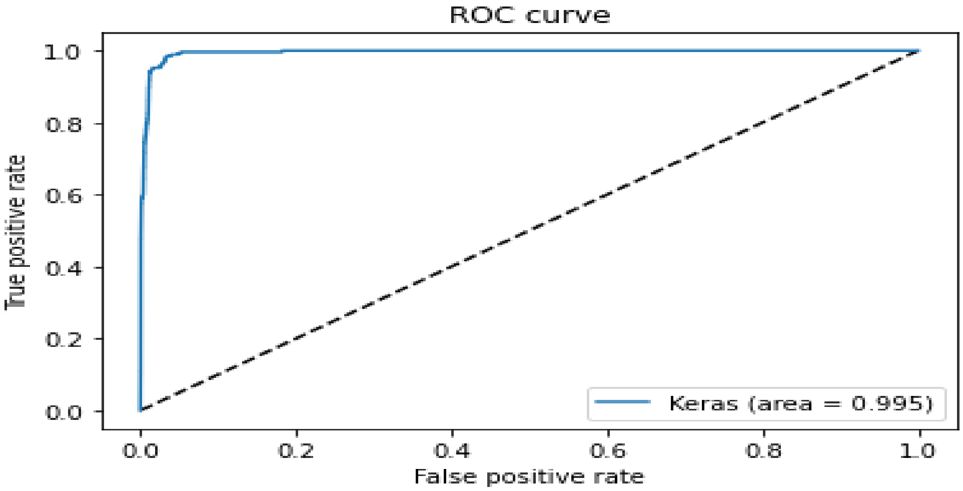
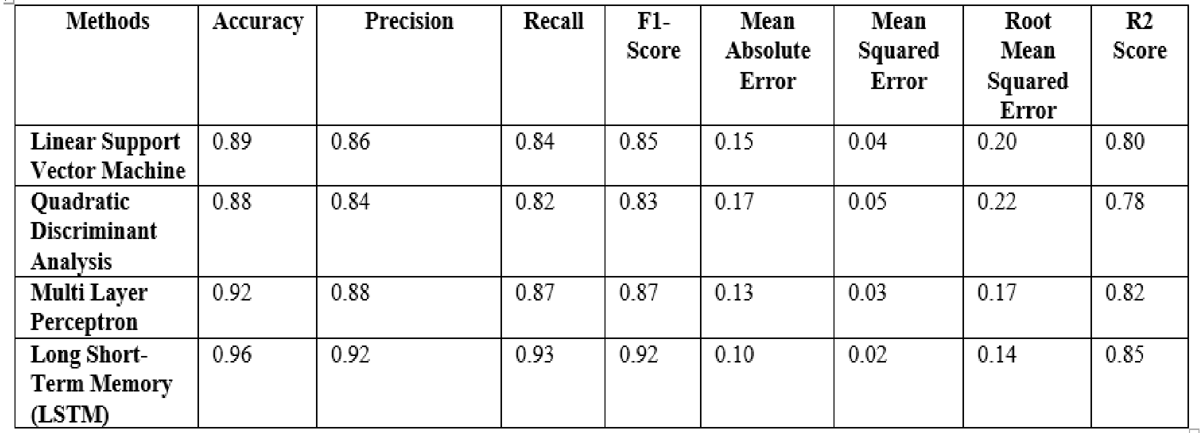


Figure 9. A model's Receiver Operating Characteristic (ROC) curve.

With an Area Under the Curve (AUC) of 0.995, the model's Receiver Operating Characteristic (ROC) curve is shown in the image.The temperature is 9 degrees below zero. The True Positive Rate (sensitivity) is plotted against the False Positive Rate in a graphical representation known as the ROC curve, which shows how well the model can discriminate between the two groups. A ROC curve quantifies the performance of a well-trained classifier by plotting the False Positive Rate on the x-axis and the True Positive Rate on the y-axis. Curves that are near to the top left corner of the plot indicate strong categorization. The AUC value for stratified columns is 0.995, which is very near to 1. This suggests a high degree of efficacy and a minimal amount of classification mistakes. A big area under the receiver operating characteristic (ROC) curve indicates a true positive.

4.4 Comparative result of models

Table 1. Findings from comparing these models.



Methods	Accuracy	Precision	Recall	F1-Score	Mean Absolute Error	Mean Squared Error	Root Mean Squared Error	R2 Score
Linear Support Vector Machine	0.89	0.86	0.84	0.85	0.15	0.04	0.20	0.80
Quadratic Discriminant Analysis	0.88	0.84	0.82	0.83	0.17	0.05	0.22	0.78
Multi Layer Perceptron	0.92	0.88	0.87	0.87	0.13	0.03	0.17	0.82
Long Short-Term Memory (LSTM)	0.96	0.92	0.93	0.92	0.10	0.02	0.14	0.85

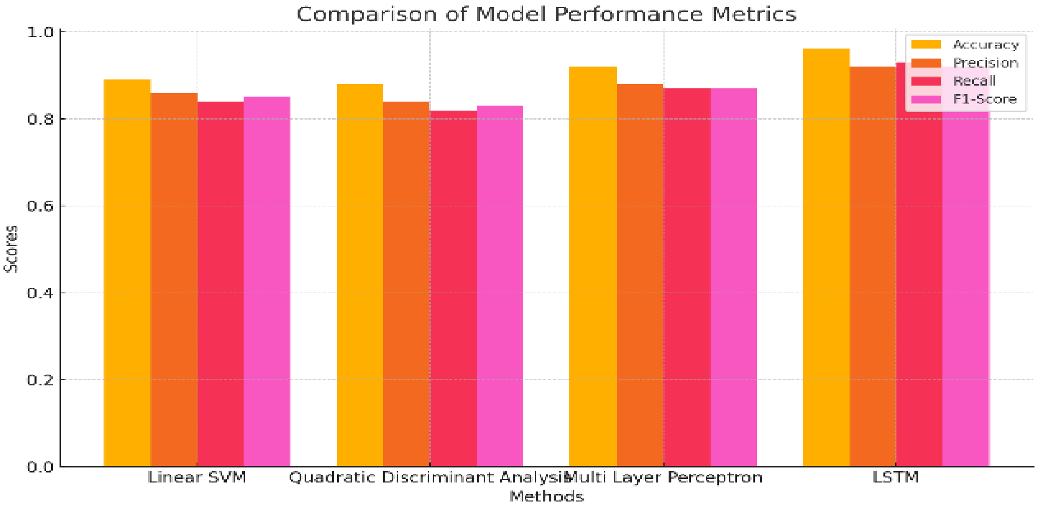


Figure 10. Comparative results of these models

Figure 10 shows the Accuracy, Precision, Recall and F1-Score of four machine learning techniques; (Linear Support Vector Machine), QDA(Quadratic Discriminant Analysis), MLP(Multi-Layer Perceptron), LSTM(Long Short-Term Memory). By all metrics, the LSTM model outperforms other methods in which it has a higher score compared to them; moreover, Multi-Layer Perceptron come as second model handle this issue. The result is that they provide slightly lower but competitive performance compared to linear SVM and Quadratic Discriminant Analysis. Visually LSTM, is clearly the best classification method for this data set considering it has better metrics in all areas which are shown based on that chart.

CONCLUSION

Applications of Deep Learning Methodologies in Intrusion Detection Systems (IDS) By using various models it reveals significant benefits. In the work examined, Long Short—TermEN Memory (LSTM) beats every competing method such as Linear Support Vector Machine (SVM), Quadratic Discriminant Analysis and Multi-

Layer PerceptronMLP in all main metrics. LSTM results in the highest accuracy (0.96), precision (0.92), recall (0.93) and F1_score (0.92) while also low errors, as suggested by lowest Mean Absolute Error (.10), Mean Squared error (.02)and Root mean squared error (Mean.14). The significantly better performance of LSTM, especially in processing complex temporal patterns present within the data, underlines not only its practical benefit but also potential use as a practical manner for boosting detection power amongst IDS standards trying to capture more advanced network landscapes.

REFERENCES

[1] G. Logeswari, S. Bose, and T. Anitha, "An intrusion detection system for SDN using machine learning," Intelligent Automation & Soft Computing, vol. 35, no. 1, pp. 867-880, 2023.

[2] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, and R. M. Mohammad, "Intrusion detection system using feature extraction with machine learning algorithms in IoT," Journal of Sensor and Actuator Networks, vol. 12, no. 2, p. 29, 2023.

[3] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," Information, vol. 14, no. 1, p. 41, 2023.

[4] S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," Computer Communications, vol. 199, pp. 113-125, 2023.

[5] A. Verma and V. Ranga, "On evaluation of network intrusion detection systems: Statistical analysis of CIDDS-001 dataset using machine learning techniques," Authorea Preprints, 2023.

[6] A. Alotaibi and M. A. Rassam, "Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense," Future Internet, vol. 15, no. 2, p. 62, 2023.

[7] A. Pinto, L. C. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure," Sensors, vol. 23, no. 5, p. 2415, 2023.

[8] A. Henry et al., "Composition of hybrid deep learning model and feature optimization for intrusion detection system," Sensors, vol. 23, no. 2, p. 890, 2023.

[9] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree," IEEE Access, 2023.

[10] A. Awajan, "A novel deep learning-based intrusion detection system for IoT networks," Computers, vol. 12, no. 2, p. 34, 2023.

[11] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, "A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things," Computational Intelligence and Neuroscience, 2023.

[12] V. Hnamte and J. Hussain, "DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system," Telematics and Informatics Reports, vol. 10, p. 100053, 2023.

[13] M. A. Hossain and M. S. Islam, "Ensuring network security with a robust intrusion detection system using ensemble-based machine learning," Array, vol. 19, p. 100306, 2023.

[14] H. Shah et al., "Deep learning-based malicious smart contract and intrusion detection system for IoT environment," Mathematics, vol. 11, no. 2, p. 418, 2023.

[15] S. Venkatesan, "Design an intrusion detection system based on feature selection using ML algorithms," Mathematical Statistician and Engineering Applications, vol. 72, no. 1, pp. 702-710, 2023.

[16] I. Hidayat, M. Z. Ali, and A. Arshad, "Machine learning-based intrusion detection system: An experimental comparison," Journal of Computational and Cognitive Engineering, vol. 2, no. 2, pp. 88-97, 2023.

[17] J. Jose and D. V. Jose, "Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset," International Journal of Electrical and Computer Engineering (IJECE), vol. 13, no. 1, pp. 1134-1141, 2023.

[18] A. S. A. Issa and Z. Albayrak, "DDoS attack intrusion detection system based on hybridization of CNN and LSTM," Acta Polytechnica Hungarica, vol. 20, no. 2, pp. 1-19, 2023.

[19] S. Maesaroh, L. Kusumaningrum, N. Sintawana, D. P. Lazirkha, and R. Dinda, "Wireless network security design and analysis using wireless intrusion detection system," International Journal of Cyber and IT Service Management, vol. 2, no. 1, pp. 30-39, 2022.

[20] M. U. Ullah, A. Hassan, M. Asif, M. S. Farooq, and M. Saleem, "Intelligent intrusion detection system for Apache web server empowered with machine learning approaches," International Journal of Computational and Innovative Sciences, vol. 1, no. 1, pp. 21-27, 2022.

[21] https://www.kaggle.com/datasets/hassan06/nslkdd