Grenze International Journal of Engineering and Technology, June Issue

An Advanced Network Intrusion Detection System based on Deep Learning Models

Sandhya Rani Medi[1], Nagaraju Krishna Chythanya[2], M Radha[3] and Sudeeksha Gowlikar[4]
[1,4]Bhoj Reddy Engineering College for Women, Hyderabad, India
Email: sandhya3chitumodu@gmail.com, sudeekshagowlikar@gmail.com
[2]Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India
Email: kcn_be@rediffmail.com
[3]CVR College of Engineering, Hyderabad, India
Email: marepalli.radha@gmail.com

***Abstract*— Due to the rapid growth of the technologies in networks and bulk amount of network traffic, the risk of cyberattacks has increased. Traditional signature-based security systems are inadequate to countermeasure these attacks. In order to improve the identification of hostile activity in network traffic, this study offers an intelligent Network Intrusion Identification System that combines machine learning & deep learning approaches. Using packet analysis tools, the suggested system records real-time network packets and extracts features and preprocesses structured data for efficient model training. To categorize network behaviour as normal or intrusive, there are many machine learning & deep learning models are deployed utilizing Python-based frameworks. The experimental evaluation shows that deep learning-based models obtain better detection accuracy and lower false-positive values than conventional machine learning techniques Scalability, versatility, and suitability for real-time deployment are guaranteed by the system's modular architecture. The findings show that the suggested strategy offers a reliable and effective way to protect contemporary network infrastructures from changing cyber threats.**

***Index Terms*— Networks, Intrusion Detection System, Deep Learning model, Packet Capture.**

I. INTRODUCTION

Systems are becoming increasingly susceptible to assaults because of the rapid advancement of network infrastructures, cloud-based services, and digital communication. Standard Intrusion Detection System(IDS) guidelines and early network security research indicate that traditional security methods are insufficient to address the size and complexity of modern network systems. [1], [2]. Massive amounts of diverse traffic are produced by modern networks, resulting in a complicated operational environment that is challenging to safeguard with static defence techniques. Advanced and adaptable security solutions are required to protect against cyberattacks including denial-of-service, probing, malware injection, and illegal access are becoming more sophisticated.

Network Intrusion Detection Systems, or NIDS, are vital for keeping an eye on network traffic and catching uncertain or malevolent activity.

Grenze ID: 01.GIJET.12.2.484_22

As primary IDS research has shown, conventional NIDS mostly depend on signature-based or rule-based detection algorithms, which are successful for known attack patterns but fail to notice advanced and zero-day attacks [1]. The effectiveness of the efficiency of these systems in dynamic network structures is further constrained by their normally high false-positive rates and their manual updating. By continually identifying trends in previous network data, machine learning-based NIDS can identify anomalies and new attacks much more effectively. When compared to other intrusion detection methods, these data-based methods can offer greater accuracy, scalability, and flexibility for intrusion detection systems.

The present study proposes an advanced IDS system that integrates machine learning and deep learning practices for effective intrusion finding and analysis of network traffic. In order to form an organized dataset, the system utilizes packet examination tools to record network packets in real-time and then extensively pre-processes and features them. To distinguish between typical and intrusive network performance, many classification methods are developed using Python-based frameworks. The proposed IDS system is suitable for use in real-time applications owing to its scalability and adaptability, with reduced false-positive rates. Collectively, these contributions overcome the principal disadvantages of conventional NIDS systems and present an effective solution for the protection of contemporary network structures from emerging cyber threats.

II. LITERATURE SURVEY

Rule-based and signature-based approaches were the focal point for most research on network intrusion Detection. In his research, Lunt identified the inability of rule-based systems to detect unknown Intruder attacks and proposed the first classification for intrusion detection mechanisms, proposing misuse detection and anomaly detection approaches [2]. The need for the introduction of automated learning mechanisms was identified because of the limitations faced by rule-based systems. Machine learning mechanisms were proposed for use in [3], and the authors proposed a data mining structure for intrusion detection, with the focus being on feature extraction mechanisms for network traffic and audit data. These revolutionary research works proposed the theory for smart intrusion detection mechanisms, Although they were driven by computational limitations and simplified traffic models.

The importance of standardized system architecture and methods of evaluation also increased in relation to intrusion detection system research. Guidelines for development execution, and management of intrusion detection and prevention systems were obtained from NIST Special Publication 800-94, which provided a systematic understanding of IDS components and challenges in real-world scenarios [1]. After that, Tavallaee et al. [4] observed the extensively utilised “KDD Cup 99” dataset and found serious challenges like class imbalance and duplication of data, which significantly affect the accuracy of performance evaluation in intrusion detection system research. The CICIDS dataset and methodology are used to evaluate IDS more accurately [5]. Moreover, Al Lail provided a comprehensive study showing that hybrid and deep learning-based NIDS provide better performance, but there are challenges in reducing false positives and real-time detection [6]. More realistic datasets like UNSW-NB15, which include modern-day attacks and a variety of network traffic patterns to build resilience in experiments, were introduced to overcome such challenges [7].

Deep learning-based IDS have been the focus of more recent research because of its capacity to inevitably extract intricate, high-dimensional patterns from network data. In recognizing complex and anonymous threats, Li et al. showed that deep learning models outperforms than traditional machine learning techniques [8]. Deep neural network topologies can significantly improve detection accuracy in real-time intrusion detection situations, as verified by Naseer and Saleem [9]. In a more recent study, Vinayakumar et al. examined intelligent IDS based on deep learning & demonstrated their efficiency in widespread network settings [10]. Inspired by these outcomes, the current work associates both machine learning & deep learning models with real-time packet capture to create a scalable and real network intrusion detection system.

To Understand and recognize historical relationships in network traffic data, IDS based Long Short-Term Memory(LSTM) Recurrent Neural Networks practice was suggested by Kim et al. [11] to classify the consecutive patterns, LSTM-based models to accomplish better than conventional machine learning classifiers. Recurrent Neural Networks (RNNs) are used in Yin et al.'s deep learning-based intrusion finding approach to effectively retrieve consecutive information from network data, in which the study demonstrates that RNN-based models outperformed traditional techniques in terms of detection accuracy and generalization, particularly for time-dependent attack patterns [12]. In all previous works, traditional based Intrusion Detection methods and in few CNN, RNN based methods are used. Our System uses real time packet capturing of packets in addition to machine learning & deep learning models by that accuracy of our proposed method is increased.

III. METHODOLOGY

Our proposed Advanced NIDS design and operational process is demonstrated in this section. The methodology, which focuses on real-time network traffic capturing and usage of machine learning & deep learning techniques, is fully based on the flow diagram shown in Figure 1.

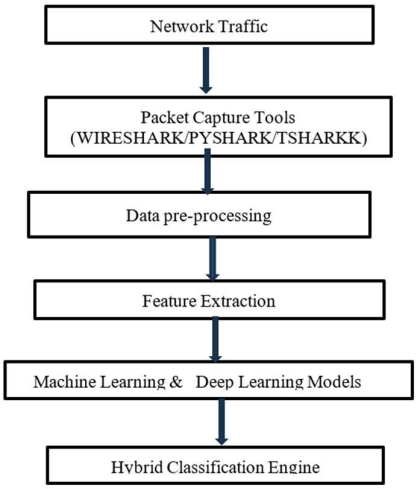

Figure 1. Flow Diagram

A. Overview of Advanced NIDS System

The proposed NIDS is a scalable and flexible approach that can monitor network traffic, analyse packet-level data, and classify network activity as intrusive or benign. Real-time packet capture, data preprocessing, feature extraction, model training, and intrusion sorting are all combined into the system. We used a hybrid learning method to take benefit of the improvements of both machine learning & deep learning models.

B. Capturing Netwotk Traffic

Using packet capture tools, network traffic is verified straight from the experiential network atmosphere. To record live packets at the network line level, the system makes use of tools like Wireshark, PyShark, and TShark. Thorough packet parameters, including protocol type, source and destination addresses, packet length, and temporal features, can be removed using these tools. The main foundation of data for intrusion detection is captured packets, which assurances that the system duplicates actual network activity.

C. Data Management and Storage

For better management and retrieval, the collected packet data is prearranged and kept in a relational database. The network traffic logs are maintained in a systematic way using a MySQL database for pre-processing and training of models. Large volumes of network data, which are shaped over time, can be easily shifted using the storage layer's capability.

D. Processing of Data

As in Network Intrusion Detection System, it is possible that the efficiency of models is severely impacted by noise, duplicate packets, and incomplete information in raw data. To resolve this problem, a preprocessing channel is provided to refine and transform the collected data. Duplicate values are removed, and categorical values are converted into numeric values. In order to ensure consistent data scaling and facilitate convergence of learning models, normalization is applied to the features.

E. Extraction of Features

To properly characterize the communication behavior, relevant features are extracted from the pre-processed network traffic. The statistical and protocol-based features, which are extracted, are related to the packet size, flow duration, and transmission frequencies, as well as flags related to protocols. The features are extracted to recognize unique patterns and abnormalities indicating malicious activities. The learned model processes the next feature vectors as input.

IV. Implementation of the Proposed Work

Python is the main programming language used in designing the entire system. Libraries like Scikit-Learn, "TensorFlow", "Keras", and "PyTorch" are used in the development of machine learning and deep learning models. Libraries like "Pandas" and "NumPy" are used in processing the data.
On the other hand, Wireshark, PyShark, and TShark are used for packet collection and analysis. Real-time intrusion detection, model development, and data management are all guaranteed through the use of all these tools.

A. Implementation of Machine Learning Model

Several types of machine learning procedures used for Intrusion Detection System classification exists. These include probabilistic and decision-based algorithms that can recognize patterns in past data related to communication networks.
Each model is trained to distinguish between normal and abnormal communications using Python-based machine learning techniques.
Each model is individually evaluated to assess its reliability and classification capabilities.

B. Implementation of Deep learning Model

Deep learning models are integrated into the system to identify complex and non-linear correlations in network traffic data.
The deep learning models are used in the development of neural network architecture to enable automatic learning of high-level representations from the obtained data. The models are adaptive to changing network behaviours since they are learned iteratively. This method improves detection accuracy and minimizes dependence on feature engineering.

C. Model Assessment and Training

For testing the model's performance, the data is divided into testing and training phases. During evaluation, the working of the model is checked against unseen data, and in training, the model is used to recognize patterns in data related to traffic. For testing the efficiency of the model in detecting data, "accuracy, precision, recall, and F1-score" are used in evaluation metrics. For making it more practical in real-world scenarios, false positives are targeted.

D. Alert Generation and Intrusion Detection

The models are used in the detection engine to inspect incoming network data after they have been skilled. In real time, every packet or flow is characterised as either invasive or normal. The system creates alerts to alert administrators when doubtful activity is found, allowing for rapid response to possible security risks.

V. Results and Discussion

The results of experiments carried out from the application of the recommended NIDS are shown in this part. The efficiency of data pre-processing, model training performance, classification accuracy, and real-time detection abilities are used to evaluate the system performance.
Real-time network packets that were logged and converted into flow-based records made up the dataset. Several statistical and protocol-associated attributes that were extracted during pre-processing were used to represent each record.

A. Data Preprocessing Results

By removing redundant and unfinished records, pre-processing significantly enhanced the quality of the data. The result of pre-processing on the recorded network traffic is briefed in Table I. Stable model training and detailed classification were made likely by the pre-processing step's reduction of noise and improvement of consistency.

Table I: Impact of Data Preprocessing

Description	Count
Raw Captured packets	52,000
Duplicate/irrelevant packets removed	7,800
Cleaned packets used for training	44,200
Extracted features per record	18

B. Model Training Performance

The cleaned dataset was used to train both deep learning & machine learning models mentioned in Figure 2. It is analysed that compared to conventional machine learning techniques, deep learning models showed reduced loss values and smoother convergence as shown in Figure 3.

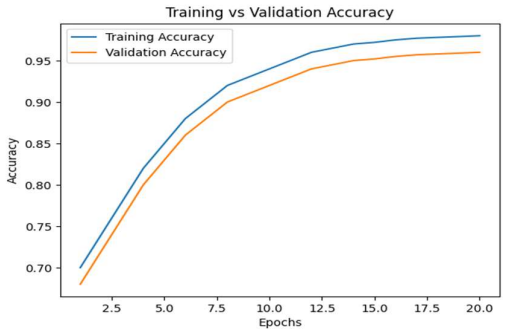

Figure 2. Training & validation accuracy curve for deep learning model Figure 3. Training loss convergence of the deep learning model

C. Classification of Performance Metrics

Accuracy and Precession are the general metrics including F1 Score, Recall used to assess individual performance of model. A comparison of machine learning models for our advanced NIDS is shown in Table II.

TABLE II: ADVANCED NIDS PERFORMANCE USING MACHINE LEARNING MODELS

Model	Accuracy (%)	Precision	Recall	F1-Score
Logistic Regression	91.4	0.90	0.89	0.89
Decision Tree	93.1	0.92	0.91	0.91
Random Forest	95.6	0.95	0.94	0.94
Support Vector Machine	94.2	0.93	0.92	0.92

D. Deep Learning Model Results

Higher detection accuracy and improved generalization on unseen data were attained through deep learning models. The performance of such models is summed up in Table III. The model's capacity to identify complex non-linear correlations in network traffic is recognized with the improvement.

TABLE III. ADVANCED NIDS PERFORMANCE USING DEEP LEARNING MODELS

Model	Accuracy (%)	Precision	Recall	F1-Score
Neural Network	97.8	0.97	0.96	0.96

E. Real Time Intrusion Detection Results

A real-time detection pipeline was implemented using the learned models. When aberrant behaviour was found, intrusion alarms were created based on the dynamic analysis of incoming network packets.
Important findings:

- For real-time monitoring, the average detection latency stayed within reasonable bounds.
- There was a high degree of consistency in identifying intrusive traffic.
- The production of alerts was accurate and timely.

F. False Positive and False Negative Analysis

For real-world usage, dropping false warnings is vital. The Table IV records occurrences of false positives observed during testing along with the false negatives. The deep learning model enhanced system consistency by showing a significant reduction in false alerts. The deep learning model improved system dependability by showing a significant decrease in false alerts.

TABLE IV: FALSE ALERT ANALYSIS

Model Type	False Positive Rate (%)	False Negative Rate (%)
Machine Learning	5.1	4.3
Deep Learning	2.2	1.9

VI. CONCLUSIONS

Our work presented an advanced Network Intrusion Detection system that uses hybrid deep learning & machine learning mechanisms to provide higher accuracy and less false positive rates. Data pre-processing and extraction of features was done by considering network traffic and packet-level information in real time as parameters. The proposed solution's scalability and flexibility is achieved by the use of real-time packet capture tools and an integrated system design. It also verifies the invasive behaviour of network traffic while maintaining realistic response times which is suitable for deployment of our model in the real world. Overall, the developed NIDS offers a trustworthy and well-organized method for identifying damaging activities in modern networks. Our proposed deep learning approach for IDS shows 97.8% accuracy which is more compare to existing machine learning models. Finally, the results validate that how data-driven intrusion detection procedures can improve cybersecurity methods against unpredictable threats.

REFERENCES

[1] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, National Institute of Standards and Technology, 2007.

[2] T. F. Lunt, "A Survey of Intrusion Detection Techniques," Computers & Security,vol.12, no.4, pp. 405–418, 1993.

[3] W. Lee and S. J. Stolfo, "A Data Mining Framework for Building Intrusion Detection Models," in Proceedings of the IEEE Symposium on Security and Privacy, 1999, pp. 120–132.

[4] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009.

[5] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proceedings of the International Conference on Information Systems Security and Privacy,2018.

[6] M. Al Lail, "Machine Learning for Network Intrusion Detection: A Comprehensive Review," Future Internet, vol. 15, no.7,2023.

[7] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," Military Communications and Information Systems Conference, 2015.

[8] Y. Li, R. Ma, and R. Wang, "Intrusion Detection Using Deep Learning," IEEE Communications Surveys & Tutorials, vol.21,no.3,pp.2052–2073,2019.

[9] M. Naseer and Y. Saleem, "A Deep Learning Approach for Intrusion Detection System," Future Generation Computer Systems, vol.90,pp.94–104,2019.

[10] R. Vinaya kumar et al., "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp.41525–41550,2019.

[11] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, South Korea, 2016, pp.1–5.

[12] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, vol. 5, pp. 21954–21961, 2017.