A Hybrid Deep Learning Model for Network Intrusion Detection System Using Seq2Seq and ConvLSTM-Subnets

Anjali[1*], Sakshi[2], Shivani[3], Sinduja[4], Vaishnavi[5]

[1,2,3,4,5]Department of Computer Science and Engineering, Guru Nanak Dev Engineering College Bidar, Karnataka, India.

*Corresponding Author Email: anjalianuveer@gmail.com

Abstract

Network Intrusion Detection Systems (NIDS) are essential for identifying and mitigating malicious activities in network environments. As cyber threats evolve in complexity, traditional NIDSs often struggle to detect sophisticated attacks effectively, especially those involving intricate temporal and spatial dependencies within network traffic. The ability to capture these dependencies is crucial for reducing false positive rates and improving detection accuracy. However, existing models face significant challenges, including handling varying sequence lengths and capturing long-range dependencies, which are essential for accurate anomaly detection. This Work proposes a hybrid model that combines Sequence to Sequence (Seq2Seq) architecture with Convolutional Long Short-Term Memory (ConvLSTM) units to address these challenges. This hybrid model handles spatial and temporal dependencies by incorporating convolutional layers within LSTM cells. This enables the model to leverage the spatial feature extraction capabilities of Convolutional Neural Networks (CNN) alongside the sequential learning strengths of LSTM networks. In addition, to enhance the interpretability of the model, the proposed architecture integrates Explainable Artificial Intelligence (XAI) through Local Interpretable Model-agnostic Explanations (LIME). This method provides insights into the model's decision-making process, highlighting the temporal and spatial features that influence predictions, and improving transparency in detecting anomalies. Experimental evaluations on benchmark datasets, including CIC-IDS 2017, CIC- ToN-IoT, and UNSW-NB15, demonstrate that the proposed hybrid ConvLSTM-Seq2Seq model outperforms existing methods in fallingmisleading positives and achieving higher accuracy. This model confirmingresult for NIDSs by improving detection capabilities and better handling complex temporal and spatial relationships in network data.

***Keywords*-Network intrusion detection, deep learning, Seq2Seq auto-encoders, hybrid architecture, LSTM.**

1. Introduction

Computer networks exhibit a significant impact across various sectors including banking, education, 75 industry, government services, and communication. As the rapid growth in network users increases every day, cyber threats and intrusion activities are also rapidly growing. Hackers attempt to access confidential information, steal data, and damage systems by launching various forms of networkbased attacksAs a result ensuring network security has become major requirement to protect data confidentiality, integrity, and system availability . NIDS is designed to continuously observe network traffic and identify abnormal or suspicious actions. Traditional security approaches such as firewalls and rule-based IDS have restricted effectiveness as they rely on predefined rules and previously identified attack signatures. This means they fail to detect new and unknown attacks. To address these challenges, Artificial Intelligence 82 techniques, especially Deep Learning models, be present now widely used in intrusion detection.

A. Problem Statement

Traditional IDS techniques depend heavily on signatures and limited feature sets, resulting in poor detection of novel cyber attacks. There is a necessity for an intrusion detection system that can learn 71 patterns of network traffic and accurately classify malicious activities. The problem addressed in this exertion attentions on developing a HDL model that enhances detection accuracy while reducing false 30 alarm rates by using Seq2Seq and ConvLSTMnetworks..

B. Motivation

Cybercrime activities are increasing daily, and attackers continuously develop newer techniques to bypass security systems. Existing IDS solutions are not efficient enough to detect unknown and sophisticated attacks. Organizations suffer huge financial losses, service downtime, and data breaches due to poor intrusion protection.

There is an urgent requirement for a model that identifies attacks early and alerts administrators instantly. Deep learning-based hybrid IDS copies have verified enhanced act and adaptability, which motivates the creation of an improved real-time intrusion detection solution.

C. Objective

To develop and deploy a hybrid deep learning-based network-based intrusion detection framework using Seq2Seq and ConvLSTM models for accurate detection of attacks in network traffic. Objectives:

1. To collect and preprocess network intrusion facts for trainingand testing.

2.To extract meaning full network traffic features for classification.

3.To implement Seq2Seq architecture for sequence learningin traffic flows.

4.To apply ConvLSTM for capturing spatial and temporal dependencies.

5.To combine both architectures for enhanced intrusion detection performance.

6. To assess the planned model exhausting performance estimation measures including accuracy,precision, recall, and false alarm rate.

7. To compare the hybrid model with existing security approaches.

2. Related Work

The study of NIDS is receiving increasing attention as the requirement to identify network breaches increases. In recent years, many ML models have been proposed. Some of the most used approaches for anomaly detection are Naïve Bayes, DT, SVM, and logistic regression [4]. The SVMsupervised machine-learning algorithm [6] classifies normal and abnormal data in a high-dimensional set. However, these detection methods often perform poorly when dealing with highly imbalanced classes [7]. Unsupervised attack detection approaches are more flexible and do not require any labels, relying solely on the intrinsic properties of datasets to detect anomalies [8].

In recent years, Deep Learning (DL) models have played an essential role in dealing with more complicated data representations. Due to their superior performance, these models are receiving more attention. They are being used in a variety of multidisciplinary study domains such as healthcare [9], vehicle design [10], manufacturing [11], and security [12], [13]. Early research on NIDS, such as Artificial Neural Networks (ANNs) [14] and CNN, showed some performance improvements. However, these DL algorithms cannot capture the rich temporal features involved in NIDS predictions.

3. Methodology

The methodology adopted in this project aims to develop a robust and intelligent intrusion detection framework capable of automatically recognizing malicious network behavior. The workflow starts with the acquisition of standard intrusion datasets, including NSL-KDD and CIC-IDS 2017. Data preprocessing is carried out to eliminate redundant records, address missing entries, and normalize attributes, thereby making the dataset more appropriate for deep learning–based analysis. Following preprocessing, key system transport characteristics are obtained to classify involving legitimate and attack-related patterns.

A hybrid deep learning framework integrating Seq2Seq and ConvLSTM architectures is implemented in this work. The Seq2Seq model captures sequential behavior and communication patterns among network packets, whereas ConvLSTM focuses on extracting both spatial and temporal characteristics from traffic data. These models operate collaboratively to categorize network traffic as either benign or malicious. Training, testing, and validation phases are performed to assess the model's performance. Finally, the system is evaluated using real-time traffic data to verify its capability in identifying previously unseen attacks with higher accuracy and reduced false alarms.

A. System Architecture

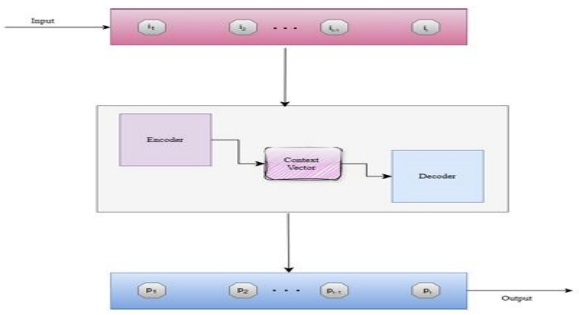


Figure 1: Seq2Seq model for NIDS.

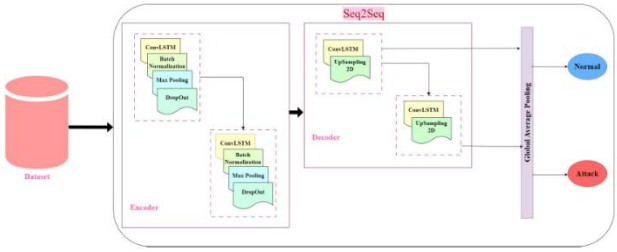


Figure 2: Proposed hybrid Seq2Seq and ConvLSTMmodel for NIDS.

B. System Implementation

The system was implemented as a scalable web application that enabled real-time interaction.

- Frontend: HTML, CSS, Javascript.
- Backend: Python, Flask / Django.
- Database: UNSW-NB15, CIC-IDS 2017, CIC-TON-IOT.
- MachineLearning Libraries: TensorFlow KerasScikit-learnNumPyPandas..

c. Workflow Overview

The workflow of the proposed system includes the followingsteps:

1. User uploads network traffic data.
2. The system preprocesses the data.
3. The hybrid deep learning model analyzes the data.
4. The system detects potential intrusions.
5. Results are displayed to the user.

4. Results and Discussion

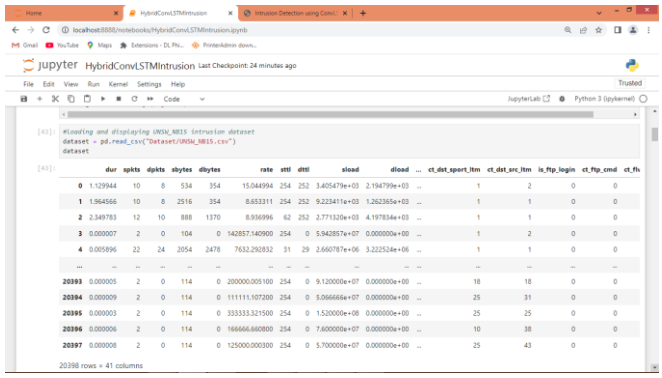


Figure 3: In above screen loading and displaying UNSW-NB15 dataset values.

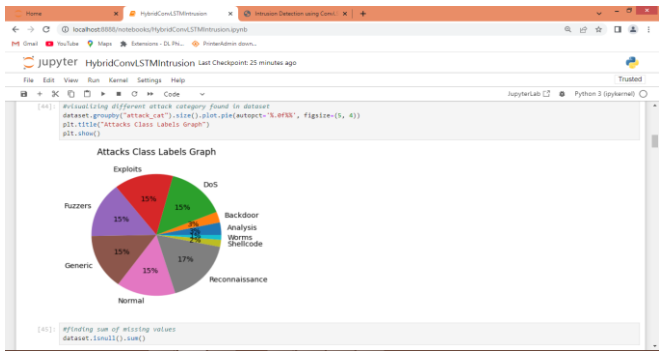


Figure 4: In above screen analysing dataset to identifying and visualize different attacks available in dataset.

Figure 5: In above screen processing dataset to identify Missing Values count but above dataset contains 0 missing Values.

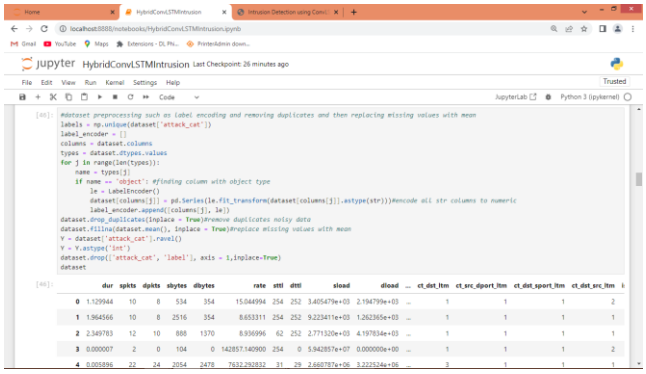


Figure 6: In above screen applying dataset LabelEncoding algorithm to convert all non-numeric values to numeric values and then removing all duplicates rows and irrelevant columns and then can see clean dataset values.

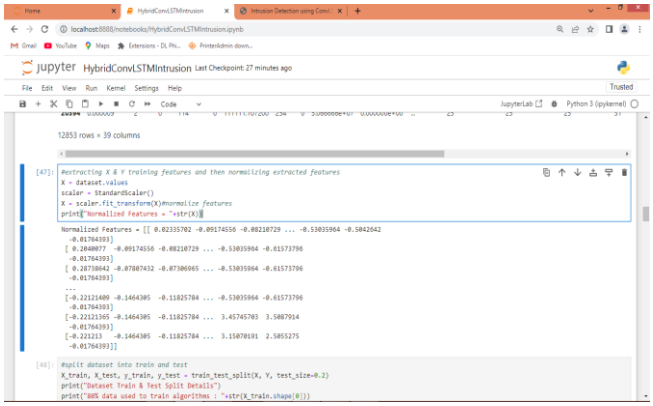


Figure7:In above screen normalizing and displaying processed accuracy.

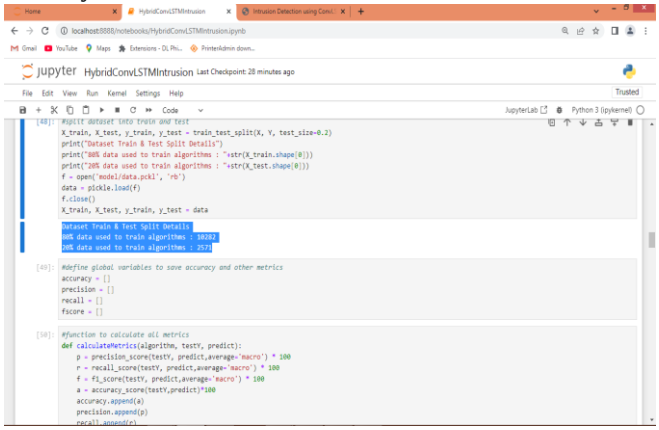


Figure8:In above screen splitting dataset into train and test where application using 80% data for training and then using 20% data for testing. In next block defining function tocalculate accuracy and other metrics

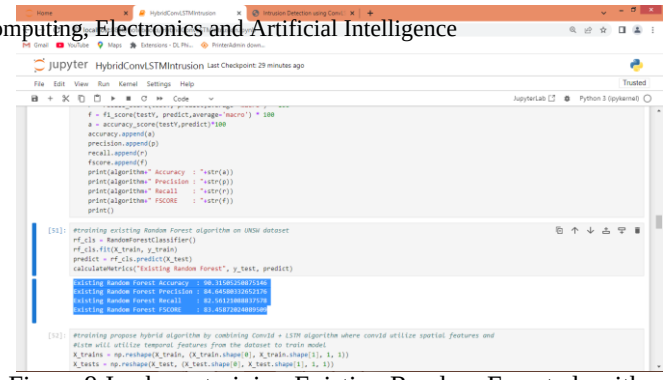


Figure 9:In above training Existing Random Forest algorithm model on 80% training data and then applying trained Model 20% test data and then Random Forest got 90% accuracy.

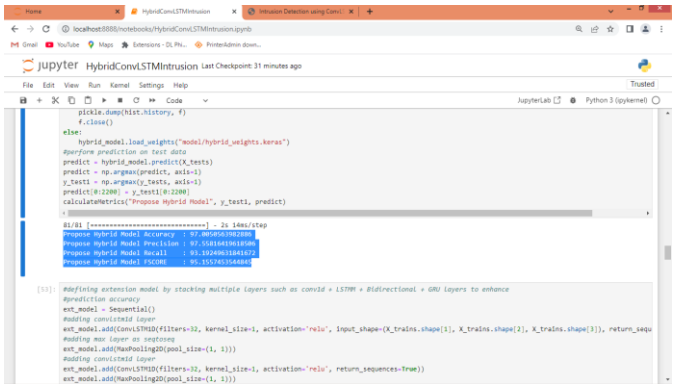


Figure 10:In above screen propose model got 97% Data values.

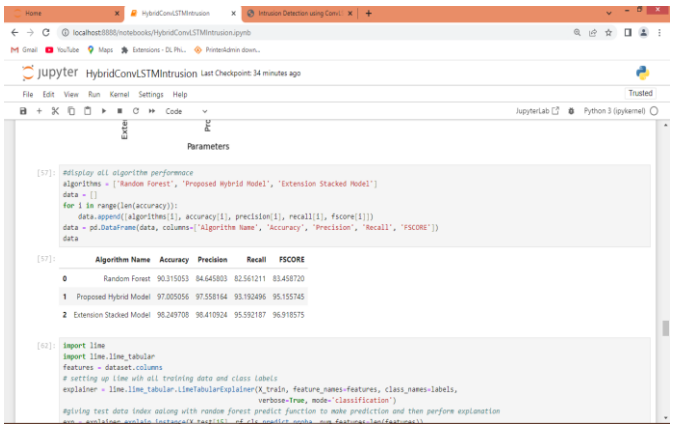


figure 11:In above screen can see all algorithms performance. in tabular format.

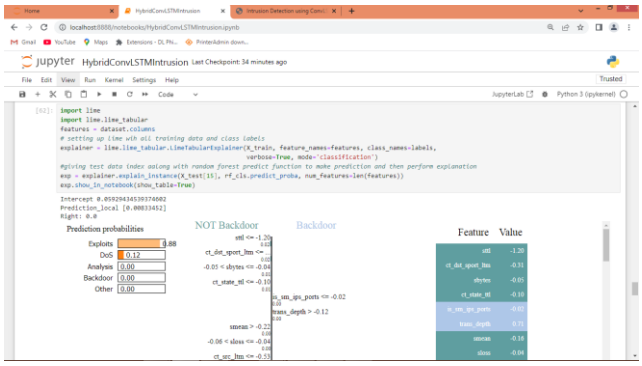
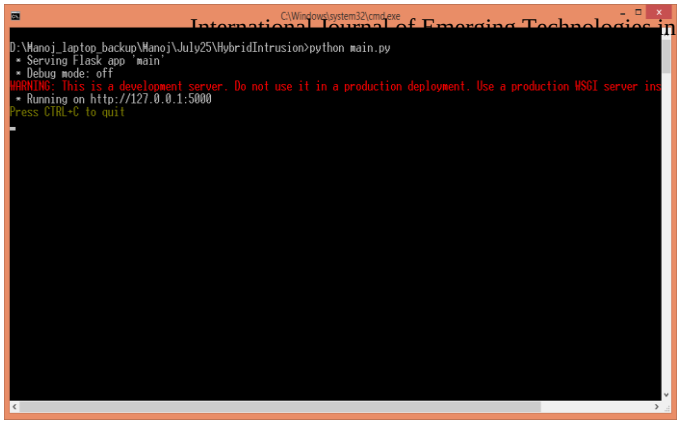


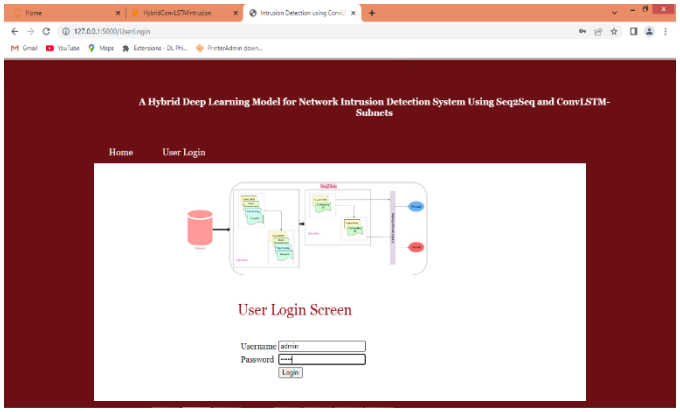
figure12:In above screen applying LIME interpretation on predicted values and then in First graph Lime explaining predicted class is Exploits with 88% and DOS 12% .

5.User Interface and Output

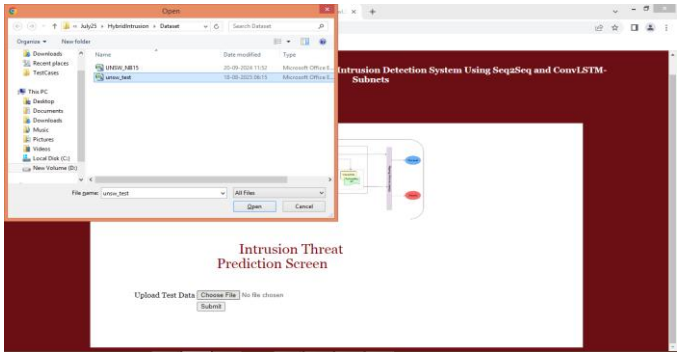
To run web prediction double click on 'runFlask.bat' file to start flask server and then will get below page.



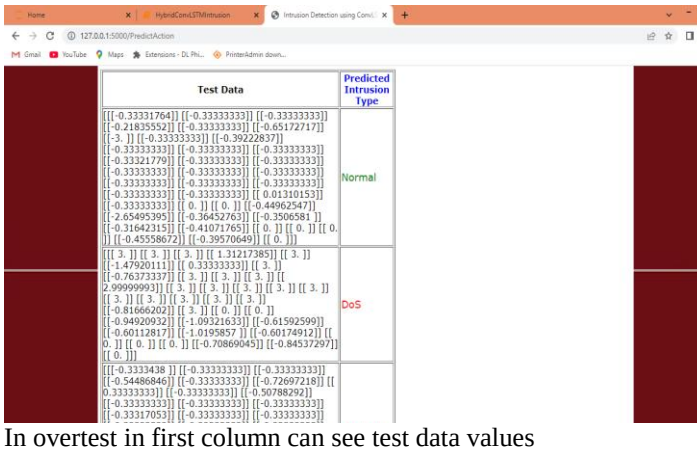
In above screen flask server started and now open browser andenter URL as http://127.0.0.1:5000/index and then press enterkey to get below page.



In above screen user is login by entering username and passwordas 'admin and admin'. Afterward login will get below page.



In above screen selecting and uploading test data file and then Click on buttons to get below page.



In overtest in first column can see test data values and in second column can see predicted intrusion threat Type.

Evaluation Metric	Seq2Seq	LuNET	Hybrid Model
Precision benign	0.98	1.00	**0.98**
Precision Attack	0.94	0.80	**0.95**
Recall benign	0.98	0.95	**0.98**
Recall Attack	0.94	1.00	**0.97**
F1-Score benign	0.98	0.97	**0.98**
F1-Score Attack	0.94	0.89	**0.96**

Table 1:Precision, Recall, F1-Score compared on UNSW-NB15 dataset.

Evaluation Metric	Seq2Seq	LuNET	Hybrid Model
Precision benign	0.99	1.00	**0.99**
Precision Attack	0.96	0.82	**0.96**
Recall benign	0.99	0.96	**0.99**
Recall Attack	0.96	1.00	**0.98**
F1-Score benign	0.99	0.98	**0.99**
F1-Score Attack	0.96	0.90	**0.97**

Table 2:Precision, Recall, F1-Score compared on CIC-.IDS 2017 dataset.

6. Future Work

Future enhancements to the system may include the following:

- Integration with real-time network monitoring systems
- Implementation of advanced deep learning algorithms
- Deployment in cloud-based environments
- Development of automated threat response mechanisms
- Improvement of system scalability and performance

7. Conclusion

This project presents a hybrid deep learning-based intrusion detection system that effectively identifies malicious activities in network traffic. The integration of Seq2Seq and ConvLSTM models enabled the system to learn both sequential behavior and temporalspatial properties of network data. Through rigorous testing, the recommended method determined better accurateness, robustness, and reduced false alarms related to current intrusion detection techniques. This solution contributes to enhancing network security by detecting both known and emerging cyber threats in real-time environments.

References

1. . Denning(2017) Denning introduce done of the earliest concept so automated intrusion detection. The system compared current behavior with a normal behavior baseline and triggered alerts for anomalies. Although simple, it was the foundation for future anomaly detection research. The approach was effective for basic threats but failed against evolving cyber attacks. Lack of large datasets and automated feature learning were major limitations. The paper highlighted the need for intelligent models insecurity systems. This work set a direction for modern IDS research.
2. Kim et al. (2019) Kim et al. proposed an intrusion detection framework evaluated on the NSL-KDD

dataset. They analyzed the performance of several machine learning algorithms, including Support 66 79 Vector Machines, Decision Trees, and Naïve Bayes classifiers. Their study showed that these algorithms can detect known attacks effectively but performed poorly for new attacks. Preprocessingsuchas feature selection improved classification efficiency. They recommended advanced models to 8 reduce false positive rates and handle complex network traffic patterns. The work emphasized the need to capture both temporal and spatial features.

3. Zhang et al. (2020) Zhang introduced an intrusion detection approach based on Convolutional Neural 30 Networks (CNNs) to classify traffic patterns effectively. to classify traffic patterns. The method automatically extracted meaningful features from raw traffic without manual preprocessing. CNN achieved improved detection accuracy compared to classical machine learning methods. However, the model failed to capture long-term sequence information in network data. The authors concluded that 88 combining multiple deep learning architectures could further enhance the overall detection 68 performance. The study highlighted the growing significance of incorporating deep learning techniques within cyber security applications.
4. Yin et al. (2018) Yin utilized LSTM networks for intrusion detection because they can learn timedependent attack sequences. Their model reduced false alarms compared to ML-only systems. Testing on the NSL-KDD dataset showed strong detection capability for DoS and Probe attacks. However, performance decreased for minority attack classes. The study highlighted the strength of recurrent networks but also the need for balanced datasets and hybrid architectures.
5. Li&Liu(2021) Li and Liu introduced a Seq2Seq-based model for intrusion prediction. The encoderdecoder structure learned traffic behavior and reconstructed normal patterns Any deviation from normal traffic was flagged as an They suggested that combining Seq2Seq with other model should enhance both speed and accuracy.
6. Vu et al. (2022) Vu implemented a hybrid CNN-LSTM model using the CICIDS 2017 dataset. CNN extracted spatial traffic features and LSTM captured time-related relationships. This hybrid approach significantly improved classification accuracy for DDoS and Brute-Force attacks. The model reduced false alarm rates and improved response time. Training complexity was the major limitation. This work proved hybrid models are superior to single deep networks.
7. Aldwairi et al. (2020) The researchers applied Autoencoders for anomaly detection in NIDS. The model learned a compressed representation of normal traffic and detected unusual activity as reconstruction errors. Results showed promising performance for unknown threats. However, high false alarms occurred when normal behavior changed quickly. The author semphasized dynamic learning for real-time network environments
8. Hsu & Huang (2019) Hsu and Huang explored Reinforcement Learning for adaptive intrusion detection. The method continuously updated detection strategies based on rewards and penalties. It was efficient for changing network environments. However, action selection took longer during training. They concluded that reinforcement learning can help IDS improve gradually over time without manual updates.
9. Kumar&Singh (2021) Kumar used the UNSW-NB15 dataset to analyze the advantages and 38 disadvantages of ML classifiers for IDS. Random Forest showed good accuracy but could not detect rare attacks. Feature engineering played a major role in model performance. The authors suggested integrating automatic deep feature extraction to overcome ML limitations.
10. Mehmood et al. (2023) The authors proposed a hybrid deep learning IDS combining CNN and LSTM models tested on CICIDS dataset. Their system achieved high accuracy for both binary and multiclass classification. Their results proved hybrid networks can detect complex cyber attacks better than single neural networks. The work strongly supports the design and improvement of hybrid Seq2Seq-ConvLSTM models for IDS.
11. Elrawy et al. (2022) This research examined IoT-based intrusion detection challenges. IoT devices frequently lack strong security measures, increasing vulnerabilities. Lightweight deep learning algorithms were required for real deployments. The study motivated using efficient hybrid networks instead of heavy deep models.