Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Enhanced Hybrid Seq2Seq-ConvLSTM Network Intrusion Detection System with Real-Time Alerts

Ragireddy Sreya Reddy[1], Dr. P. Prashanth Kumar[2], Dr. V. Anantha Krishna[3], Dr. U. Srilakshmi[4]

[1]M.Tech, [2]Associate Professor, [3]Professor, [4]Professor & HOD
Department of Computer Science and Engineering1234
Sridevi Women's Engineering College, Hyderabad, Telangana, India

Abstract

The growing number of cyber-attacks has been emphasising the importance of intelligent and efficient Network Intrusion Detection Systems (NIDS). Traditional intrusion detection methods are ineffective against unknown attacks and have difficulty with processing large-scale network traffic. For accurate and reliable intrusion detection, this paper proposes an Enhanced Hybrid Seq2Seq–ConvLSTM Network Intrusion Detection System. The proposed model is composed of the power of sequence learning of Seq2Seq and the temporal feature extraction of ConvLSTM, enhancing the attack classification performance. To make the system more useful in practice the following features are embedded in the framework: Real-Time Alert Notification, Network Traffic Visualization, LIME based Explainability, dynamic multi-dataset support and an interactive Model Metrics Dashboard. The proposed system is tested with three data sets, namely CIC-IDS2017, UNSW-NB15 and CIC-ToN-IoT. The experimental results show that the detection performance is high, showing the improvement of the Accuracy, Precision, Recall, and F1-Score, and reducing the false positive values and false negative values. The proposed framework will be efficient, explainable, and scalable for real-time network intrusion detection, suitable for a modern cybersecurity application.

Keywords — Network Intrusion Detection System (NIDS), Seq2Seq, ConvLSTM, Deep Learning, Cybersecurity, LIME Explainability, Real-Time Alert Notification, Network Traffic Visualization.

1. Introduction

Internet technologies and digital communications have grown rapidly, causing high volume of network traffic with more cyber attacks. Thus, the security of computer networks has become an important concern for organizations and individuals. Traditional Network Intrusion Detection Systems (NIDS) are mostly signature-based and traditional machine learning methods that are not able to detect unknown attacks and process huge amount of dynamic network traffic. The recent progress of deep learning has offered better solutions based on the automatic learning of complex patterns from network data, which enhances the performance of intrusion detection.

In this paper, an Enhance Hybrid Seq2Seq–ConvLSTM Network Intrusion Detection System (NHSI) for intelligent and reliable intrusion detection is proposed. The proposed system will leverage the best of both the Seq2Seq and the ConvLSTM models to accurately classify

A. Objectives

The objectives of the project are as follows:

- Design an improved Hybrid Seq2Seq–ConvLSTM network intrusion detection system to achieve precise intrusion detection.
- To enhance network security by incorporating Real-Time Alert Notification to detect malicious activities in real-time.
- To give Network Traffic Visualization for effective monitoring and analysis of network traffic.
- To include LIME Explainability for more transparent and interpretable model predictions.
- Dynamic processing of multiple datasets of benchmark data such as CIC-IDS2017, UNSW-NB15, and CIC-ToN-IoT.
- Compare the proposed system with the reference system using performance measures like Accuracy, Precision, Recall, F1 Score, Confusion Matrix.

B. Model Diagram

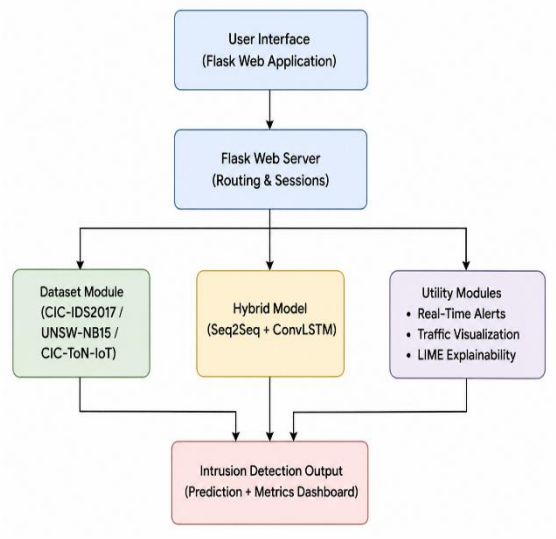

Fig. 1: Model Diagram

2. Literature Review

With the ever-growing volume of cyber-attacks and network traffic, Network Intrusion Detection Systems (NIDS) have become an integral part of the modern cybersecurity landscape. Most traditional IDS solutions use signature-based and rule-based intrusion detection techniques, which are good at detecting known attacks but poor at detecting unknown and zero-day attacks. To address these constraints, alternative solutions based on machine learning and deep learning to automatically learn complex patterns from network traffic with the aim of bettering intrusion detection accuracy have been explored.

The recent studies reveal that deep learning architectures like Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU) and Hybrid architectures bring a significant level of improvement in intrusion detection performance. One of these methods, the Hybrid Seq2Seq–ConvLSTM, is capable of exploiting both the sequence information and temporal features to enhance attack classification performance. The model has achieved good performance in some standard datasets like CIC-IDS2017 and UNSW-NB15. Current solutions, however, have been developed primarily for the purpose of enhancing classification accuracy and offer only limited support for practical deployment capabilities like real-time monitoring, visualization, and explainability.

As trustworthy AI becomes more and more important, Explainable AI (XAI) methods like LIME have been designed to explain the predictions of deep learning models by pinpointing the most important features contributing to the classification decisions. Likewise, real-time alert notification systems and visualization dashboards of network traffic are also useful features that enhance the security monitoring process and facilitate prompt reaction to threats in the network. In spite of these developments, numerous intrusion detection systems are offered as disjointed features, uncorrelated with one another and with a lack of integration.

3. Problem Statement

It is extremely difficult to make a precise intrusion detection system as network traffic increases rapidly and cyber attack methodologies become increasingly complex. Most traditional NIDS, and the recently proposed NIDS based on deep learning, are mostly based on classification accuracy and lack necessary practical functionalities such as generating an alert in real-time, visualizing traffic, and displaying explanatory prediction results as well as interactive performance monitoring. While the proposed hybrid model, which combined sequence to sequence (Seq2Seq) and Convolutional Long Short-Term Memory (ConvLSTM), was able to learn network time series and sequential data properly, it did not develop a full system that combines real-time monitoring, LIME explainability, dashboard, and multiple datasets, etc. So, there is an urgent need to design an IDS with enhanced accuracy as well as usability, transparency, and real-time monitoring system.

4. Existing System

Numerous methods have been suggested for detecting malicious network operations, such as signature-based NIDS, anomaly-based detection systems, machine learning techniques, and deep learning based NIDS. Numerous types of techniques have already enhanced network security to detect well-known and unknown intrusions. Despite, every technique provides pros and cons and still several systems have limitation over the performance in terms of real time monitor, explain ability and usability.

A. Signature-Based IDS

System Signature-based IDS systems use signatures of known attack to identify the traffic on the network. They produce minimal false alarms and can efficiently detect the known attacks with great precision. But

since these are based on known signature, they cannot detect the newly developing zero-day attacks or the previously unidentifiable attacks.

B. Machine Learning and Deep Learning-Based Systems

Machine learning (ML) and deep learning (DL) models have been developed for network intrusion detection using diverse algorithms, namely Decision Trees, Random Forest, Support Vector Machine (SVM), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) and Hybrid Seq2Seq-ConvLSTM. These models are capable of auto-extracting high-level traffic patterns from network data, which makes both signature-based and anomaly-based attacks to be detected more effectively. In particular, the hybrid Seq2Seq-ConvLSTM architecture allows models to better capture the temporal and spatial aspects, thus showing excellent intrusion detection capabilities.

C. Existing Hybrid Seq2Seq–ConvLSTM Model

Existing Hybrid Seq2Seq-ConvLSTM model integrates the sequence learning capability of Seq2Seq and the temporal feature learning capability of ConvLSTM to achieve effective network intrusion detection. The model achieves good detection performance on the test data set for the network traffic classification task. But the current system focuses on the classification of attack and does not provide additional features to meet the needs of cybersecurity applications in the future, like real-time analysis, security monitoring, explanation, interactive visualization, etc.

D. Drawbacks of Existing Systems

The major drawbacks that exist among existing technologies are as follows:

- Inability to classify the zero-day & unknown attacks (ignature based systems)
- Insufficient support for real time alerts notification at the time of attack detection.
- Lack of interactive network traffic visualization to continueously observe the network.
- Lack of LIME based explainability to justify the predictions of deep learning models.
- Poorly supported for the dynamic processing of multiple benchmark data sets.
- Lack of a central dashboard to visualize Accuracy, Precision, Recall, F1-Score and Confusion matrix

5. Proposed System

The proposed system proposes an Enhanced Hybrid Seq2Seq-ConvLSTM Network Intrusion Detection System, an intelligent and effective approach for identifying malicious network traffic accurately. This system is an integration of the sequence learning abilities of the Seq2Seq model and the temporal feature learning capacity of ConvLSTM, resulting in the appropriate classification of network traffic into normal and malicious activities. Further to ensure the practical significance of the network intrusion detection system, the designed framework is enhanced with features of Real-Time Alert Notification, Network Traffic Visualization and LIME-based Explainability.

These features allow user monitoring of network traffic, intuitive interpretation of prediction results, and immediate response to potential cyber-attacks.Besides these benefits, the proposed framework facilitates the processing of multi benchmark datasets with minimum modifications in the system architecture such as CIC-IDS2017, UNSW-NB15, and CIC-ToN-IoT. In addition to these, an Interactive dashboard has also been constructed to display Prediction Results, Network Traffic, performance statistics (Accuracy, Precision, Recall, F1-Score and Confusion Matrix), which significantly enhance the usability, interpretability and overall effectiveness of the proposed Intrusion Detection system.

A. Advantages of the Proposed System

- The major advantages of the proposed system are as follows:
- High accuracy on Intrusion detection by Hybrid Seq2Seq-ConvLSTM model.
- Dynamic support on Multiple benchmark datasets.
- Real-Time Alert Notification for immediate alert generation for the attacks.
- LIME based explainability for interpreting the results of predictions.
- Interactive Network Traffic Visualization for efficient monitoring.
- Unified dashboard for evaluating performance.
- Enhanced usability and scalability in practical cyber security domain.

6. Proposed Methodology

The proposed system follows different stages for a robust method to accurately classify the malicious traffic. The workflow starts from data collection & pre-processing then training of hybrid Seq2Seq-ConvLSTM model and the classification result will be available through an Interactive Dashboard with Real-Time alert, Visualization, Explainability, and Performance evaluation report.

A. Data Collection

Our proposed system is based on three benchmark datasets such as CIC-IDS2017, UNSW-NB15, and CIC-ToN-IoT. These datasets consist of benign and attack network traffic which represent multiple types of cyber-attacks. Such utilization of three datasets makes our intrusion detection model more resilient and applicable in multiple domains.

B. Feature Extraction & Sequence Generation

Selected Features for Network Traffic are converted into sequential input format to be fed to the Hybrid Seq2Seq-ConvLSTM Model. This will preserve temporal ordering among the records of network traffic and help model learning capability.

C. Hybrid Seq2Seq–ConvLSTM Model

These sequences after the process are fed into the Hybrid Seq2Seq-ConvLSTM model. The model is a hybrid of two sequence to sequence model and convlstm model that learns the dependency on the

sequential elements, convlstm extracts time series features from network traffic. The proposed approach makes classification of the normal and abnormal traffic better.

D. Intrusion Detection

The model has been trained to decide if the incoming traffic is normal or malicious. The output from this classification leads to the accurate identification of various attack types with minimal false alerts.

E. Real-Time Alert Notification

Once the traffic is deemed malicious, the system automatically triggers a real-time notification. The alerts notify admins when an attack occurs so they can take the right security steps.

F. Network Traffic Visualization

Visualization The results are presented on an interactive dashboard which utilizes graphical chart and display to show the analysis. The dashboard will allow users to have the ability to view the current activity in the network and traffic statistics.

G. LIME Explainability

The LIME Explainability module helps us find the key features that influence each prediction of the deep learning model, thereby increasing its interpretability.

H. Performance Evaluation

Performance measures such as accuracy, precision, recall, f1-score and confusion matrix is used for testing the proposed model's performance. This will ensure that the proposed system has a robust capability to detect any intruders.

7. System Architecture

The system architecture provides a clear overview of how the proposed **Enhanced Hybrid Seq2Seq–ConvLSTM Network Intrusion Detection System** works. It illustrates the complete flow of data, starting from network traffic collection and preprocessing to intrusion detection using the Hybrid Seq2Seq–ConvLSTM model. The architecture also includes real-time alert generation, network traffic visualization, LIME-based explainability, and performance evaluation, enabling efficient detection and monitoring of cyber threats.

A. Architectural Layers

The architecture consists of the following layers:

- **Dataset Layer:** In this layer, network traffic samples are collected from three public datasets – the CIC-IDS2017 dataset, the UNSW-NB15 dataset and the CIC-ToN-IoT dataset.
- **Preprocessing Layer:** Data are collected and then cleaned, normalized, feature-selected, and seq-convoluted for the purpose of generating sequences that will be used to train and test the model.
- **Hybrid Seq2Seq-ConvLSTM Layer:** This hybrid layer takes as input the generated network traffic sequences and it is then trained to learn patterns and temporal behaviors present in such traffic samples. This model is then trained to categorize the input sample either as benign or as malicious traffic.
- **Alert and Visualization Layer:** After classifying a given traffic record as malicious, alerts are triggered. Furthermore, this layer provides a variety of visualizations that offer an overview of network traffic, alongside explanations based on the LIME methodology about why a record was labeled as malicious.
- **Performance Evaluation Layer**: Lastly, this layer provides, through the interactive dashboard, metrics on the model's performance, such as: accuracy, precision, recall, F1-Score and confusion matrix

.

B. Architecture Description

The Architecture The developed approach utilizes the following systematic workflow for intrusion detection. At first, the network traffic data is pre-processed to cleanse the data for obtaining optimal inputs for the Hybrid Seq2Seq-ConvLSTM model. Trained Hybrid Seq2Seq-ConvLSTM classifies the each record of the network as 'Benign' and 'Attack' with finding long and short range of correlations on the time series. Real-time alerts are generated immediately as it finds malicious pattern in the traffic.

Then the prediction results will be sent to the visualization and explainability modules. The Network Traffic Visualization module provides attack statistics and distribution charts. The LIME Explainability module highlights which feature(s) cause the prediction. At last, the Model Metrics Dashboard outputs the Accuracy, Precision, Recall, F1-Score and Confusion Matrix of the designed system.

C. Architecture Diagram

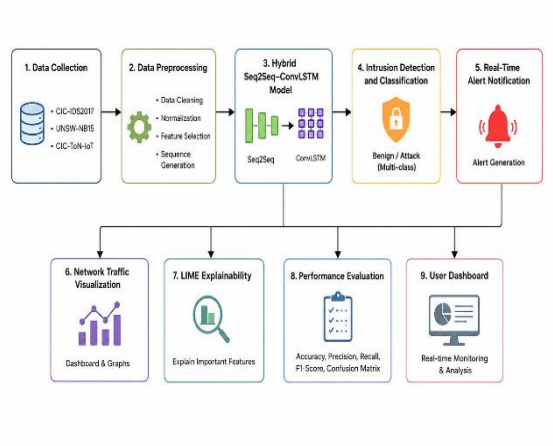

Fig. 2: Architecture Diagram

8. Design Modules

Intrusion detection system proposed is broken down into multiple working modules. This will allow the intrusion detection system to detect malicious traffic and monitoring network well. Every module will have certain functionality in order to perform its job

A. Dataset Module

The dataset module aggregates and maintains benchmark datasets utilized in the research. They include CIC-IDS2017, UNSW-NB15, and CIC-ToN-IoT datasets which feed the model during training and evaluation. The module allows loading more than one dataset which makes it versatile for assessing model performance in various network and traffic environments and under different attack patterns.

B. Data Preprocessing Module

Data Preprocessing Module - prepares the network traffic data from its original form before feeding them into the model training phase. It includes tasks of missing data imputation, duplicate removal, normalization and sequence generation. Preprocessing ensures the quality of the data by removing noise and the enhanced feature representations benefit the training of the hybrid model.

C. Hybrid Seq2Seq–ConvLSTM Module

Hybrid Seq2Seq-ConvLSTM module This module is the heart of the presented intrusion detection system. The Seq2Seq network extracts the sequential information, and the ConvLSTM network learns the spatio-temporal features. This combination improves the detection accuracy for network traffic.

D. Real-Time Alert Module

Real Time Alert Module periodically watches for output from the trained model prediction module. Whenever an indication of malicious network traffic is present, the alert will send an appropriate notification for this threat to security personnel so they can react to it.

E. Network Traffic Visualization Module

It will visually represent prediction result and traffic information through interaction Charts and Graphs in order to effectively inspect network behaviors, examine attack distributions, as well as gain more understanding about network traffic patterns.

F. LIME Explainability Module

The LIME explainability module is used for explaining predictions by the proposed Hybrid Seq2Seq-ConvLSTM model. It extracts network traffic features which have greatest impact to each prediction. Through this module, user can gain insight into the reason behind the prediction which classified record as benign or malicious. This enhances the system transparency and credibility.

G. Performance Evaluation Module

Performance Evaluation Module It evaluates the performance of the proposed intrusion detection model using several benchmark performance evaluation metrics like Accuracy, Precision, Recall, F1-Score, and Confusion Matrix.

H. Dashboard Module

Dashboard Module The proposed intrusion detection system integrates the core functionalities into an all-inclusive dashboard where the user can experience intrusions detections, alerts monitoring, network traffic visualization, LIME explanation, and model performances viainteractive chartsandevaluation matrices. Therefore, the overall system would be practical and useful**.**

9. Implementation Framework

The implementation section discusses about the software tools and the implementation process along with techniques used in designing the presented enhanced hybrid seq2seq-convlstm network intrusion detection system. It shows how the presented model is being applied and incorporated, so as to achieve an effective monitoring with accurate detection.

A. Programming Environment

We implement the proposed system with Python as it gives rich functionality in machine learning, deep learning and data mining. Interactive user interfaces are built with the use of Streamlit that helps the visualization of predictions results, traffic and network and the model's performance. The Hybrid Seq2Seq-ConvLSTM model is built with use of TensorFlow and Keras. The use of VS Studio code and Anaconda as the working environment to develop our code.

B. Libraries and Tools

The primary Libraries & Tools used in the proposed system are:

- TensorFlow and Keras - To Develop the Hybrid Seq2Seq-ConvLSTM model.
- Scikit-learn - To Preprocess data and analyze the model's performance
- Pandas and Numpy - To Load and process the dataset.
- Matplotlib and Plotly - To Visualize the network traffic and create plots.
- LIME - To explain model predictions.
- Streamlit - To Create the interactive Dashboard.
- Joblib - To save and load the training model.

C. Deployment Style

The suggested system is implemented as a local desktop application which can be hosted through Streamlit framework and accessed via web browser through which a user can detect intrusion, analyze network traffic and alerts and view the model evaluation.

C. Implementation Logic

At the implementation stage, key processes include:

1. Upload a chosen benchmark data set.
2. Pre-process the data set and normalize features.
3. Train or load a Hybrid Seq2Seq-ConvLSTM model.
4. Predict if network traffic is benign or malicious.
5. Generate an immediate alert if any attack is detected.
6. Show network traffic as a plot, and also provide explanations for decisions using LIME.
7. Compute evaluation metrics, Accuracy, Precision, Recall, F1-Score, and confusion matrix.
8. Present all output through an interactive Streamlit Dashboard.

E. Evaluation Metrics

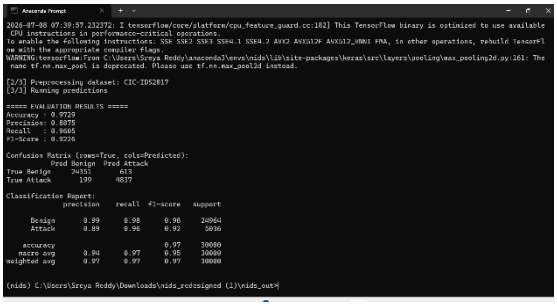

Fig. 3 Evaluation Metrics– CIC-IDS2017

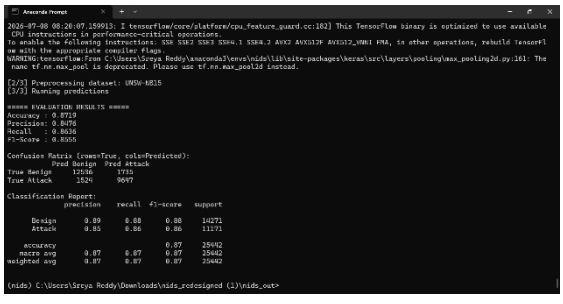

Fig. 4 Evaluation Metrics – UNSW-NB15

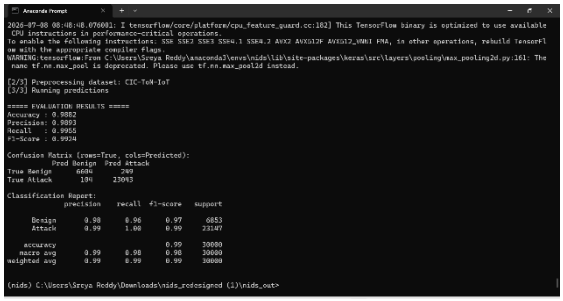

Fig. 5 Evaluation Metrics– CIC-ToN-IoT

10. Experimental Setup

In the proposed Enhanced Hybrid Seq2Seq-ConvLSTM Network Intrusion Detection System was implemented with the help of Python language using TensorFlow and Keras deep learning libraries. Implementation and running was conducted on Visual Studio Code and Anaconda environment and Streamlit was employed to build interactive dashboards to illustrate the outputs of the Intrusion Detection System. The proposed model was experimented with three benchmark data sets of network traffic: CIC-IDS2017, UNSW-NB15, and CIC-ToN-IoT.

The datasets were processed before training through missing value treatment, feature normalization and creation of appropriate input sequences to use them in the Hybrid Seq2Seq-ConvLSTM model. The proposed trained model was applied on all three datasets to check the accuracy of identifying the network traffic as benign or malicious and finally tested and results were reported using Streamlit dashboard including Accuracy, Precision, Recall, F1-Score and Confusion Matrix.

11. Testing

The system's real functionality and effectiveness are tested against a large, standard set of cyber security dataset to identify the correctness of intrusion detection and generating alert and to make it explianable under variable network traffic situations.

Table 1. Representative Test Cases

Test Case ID	Descrption	Input Type	Expected Output
TC01	Dataset Processing	Network traffic dataset	Dataset is processed successfuly
TC02	Intrusion Detection	Network traffic samples	Normal and attack traffic are classified

TC03	Alert Generation	Detected malicious activity	Intrusion alert is generated
TC04	Traffic Visualization	Network traffic data	Traffic patterns are displayed graphically
TC05	LIME Explainability	Model prediction output	Important features are identified
TC06	Dashboard Monitoring	Real-time traffic input	Live monitoring is displayed
TC07	Performance Evaluation	Test dataset	Evaluation metrics are generated

12. Results

The developed Enhanced Hybrid Seq2Seq-ConvLSTM Network Intrusion Detection System is examined based on the standard benchmark datasets (CIC-IDS2017, UNSW-NB15 and CIC-ToN-IoT). Results and validation experiments indicate the successful operation of the developed approach to detect network attacks precisely and effectively with functionalities such as real-time alert generation, visualization of network flow, and LIME explained predictions. These results confirm the accuracy and real-world usefulness of the suggested framework for intelligent network security.

A. Functional Outcomes

The presented Enhanced Hybrid Seq2Seq-ConvLSTM Network Intrusion Detection System allows classification of network traffic in both benign and malignant traffic. The introduced system gives real time alert notification, traffic visualisation and explainability for security analysis via LIME. A real time dashboard in Streamlit provides an interface for user interaction with predictions and performance monitoring. The model's validation on CIC-IDS2017, UNSW-NB15, and CIC-ToN-IoT networks shows it performs effectively across various network environments.

B. Indicative Performance Dimensions

Experimental analysis reveals that the designed system attains a respectable intrusion detection rate along with a favorable real-time performance. The integration of Hybrid Seq2Seq-ConvLSTM with notification, traffic visualization and LIME has augmented the overall functionality of the system. From three well-known benchmark datasets, the resultant metrics prove the efficiency and generalization of our model. Henceforth, a readily monitorable dashboard has been developed to monitor network traffic effectively with useful information and insights for prompt detection of the cyber attacks.

B. Result Screenshots

Note: To measure the proposed Hybrid Seq2Seq-ConvLSTM Network Intrusion Detection System's performance, it was tested on CIC-IDS2017, UNSW-NB15, and CIC-ToN-IoT datasets. In this section only representative figures of CIC-IDS2017 is represented for abbreviation, performance comparison of all datasets has already been discussed in prior.

1. NIDS Dashboard

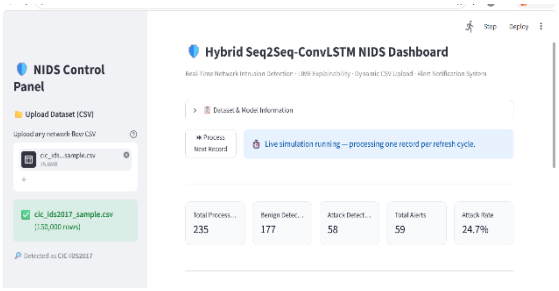

Fig. 6: NIDS Dashboard

2. Live Traffic Monitoring

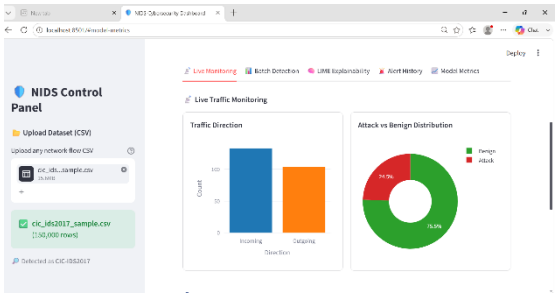

Fig. 7. Live Traffic Monitoring

1. Batch Intrusion Detection Results

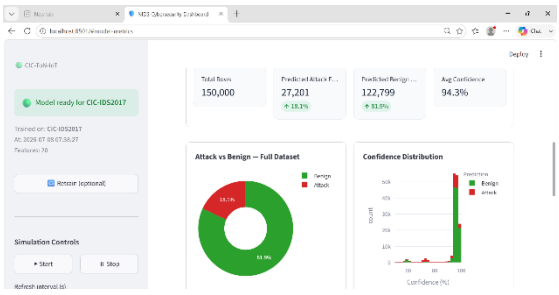

Fig. 8: Batch Intrusion Detection Results

4. LIME Explainability Results

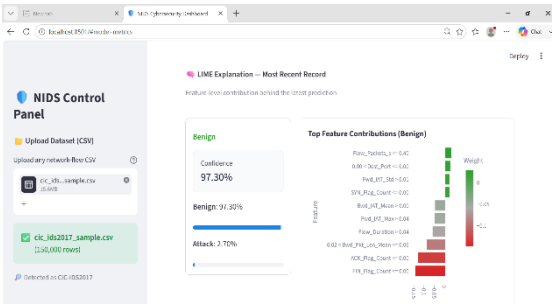

Fig. 9. LIME Explainability Results

5. Alert History Dashboard

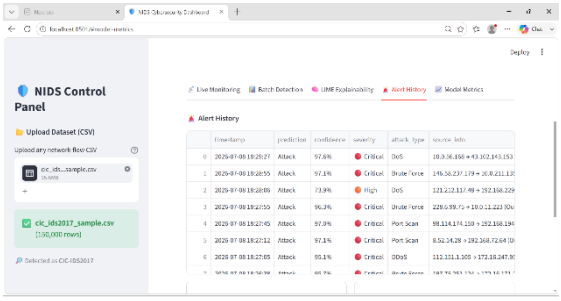

Fig. 10: Alert History Dashboard

6 . Alert Severity and Attack Distribution

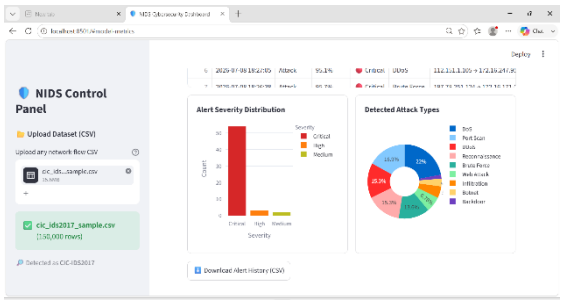

Fig. 11: Alert Severity and Attack Distribution

7. Confusion Matrix

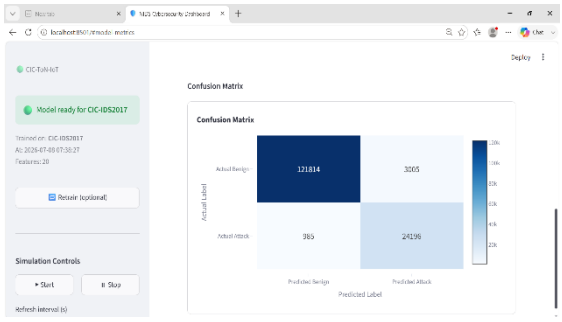

Fig. 12. Confusion Matrix

13. Results Discussion

The Enhanced Hybrid Seq2Seq-ConvLSTM Network Intrusion Detection System is tested using the three benchmark datasets: CIC-IDS2017, UNSW-NB15 and CIC-ToN-IoT. The results indicate that the proposed hybrid deep learning network can effectively distinguish between normal and malignant network traffic with high performance. As can be seen in performance parameters of three datasets, it can work in variety of network traffic while keep intrude capability consistently.

Besides efficient intrusion detection, we introduce real-time alert notification, network traffic Visualization, and LIME-based explanation into the designed system. These modules increase the applicability of our system in the cybersecurity area. A dashboard based on Streamlit is developed to facilitate the ongoing observation of the network behaviors and offer a visualization for understanding the classification results. In this way, the developed system is considered to be an efficient, understandable and practicable method to detect intrusions compared to other existing intrusion detection methods.

14. Limitations

Limitations of the suggested algorithm include the following:

- The proposed system was evaluated on benchmark datasets and is yet to be deployed and validated on a live production network.
- Performance of any model is sensitive to diversity and quality of training datasets.
- The computational overhead and time required to train Hybrid Seq2Seq-ConvLSTM are relatively large.
- The system may need to be retrained from time to time as new and novel cyber-attacks evolve.
- Computational overhead of producing the feature explanation using LIME is a non-negligible factor for the explanation generation.

15. Conclusion

Intrusion detection system based on improved Hybrid Seq2Seq-ConvLSTM Network introduced an intelligent method with deep learning technology which can detect the network intrusion successfully. According to experimental simulation on CIC-IDS2017, UNSW-NB15 and CIC-ToN-IoT benchmark dataset, the combined model of Seq2Seq and ConvLSTM can classify malicious network traffic accurately, the experiment results also shows that improved model had a credible performance under different network traffic status.

Apart from effective intrusion detection, including real-time alert notification, network visualization and LIME based explainability makes it more usable and trustworthy. A Streamlit dashboard to easily monitoring the network traffic is used for practical cybersecurity system design. In short, the developed system provided a scalable and interpretable system design for the intelligent network intrusion detection and a baseline for developing more future work of real-time and adaptive system in the cybersecurity field.

16. Future Scope

Future Directions and Extensions The developed Enhanced Hybrid Seq2Seq-ConvLSTM Network Intrusion Detection System could be extended to run in enterprise and cloud environments to detect intrusion attacks in a real-time. In addition, efforts would continue on enhancing zero-day and persistent threats through deep learning-based models and larger datasets. Moreover, integration with an automatic response to detected threats is recommended to handle detected intrusions with limited human intervention. Moreover, reducing the computation overhead and computational time with optimization, using other explainable AI techniques to interpret the results would be effective.

References

1. A. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 2018.
2. N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," in 2015 Military Communications and Information Systems Conference (MilCIS), pp. 1–6, 2015.
3. A. Vinayakumar, K. P. Soman, and P. Poornachandran, "Evaluating Deep Learning Approaches to Characterize and Classify Cyber Attacks Using Network Traffic Data," Future Generation Computer Systems, vol. 89, pp. 443–457, 2018.
4. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in IEEE Symposium on Security and Privacy, pp. 305–316, 2010.
5. Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," in Network and Distributed System Security Symposium (NDSS), 2018.
6. A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," in Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, pp. 21–26, 2016.
7. I. Sutskever, O. Vinyals, and Q. V. Le, "Sequence to Sequence Learning with Neural Networks," in Advances in Neural Information Processing Systems (NeurIPS), pp. 3104–3112, 2014.
8. X. Shi et al., "Convolutional LSTM Network: A Machine Learning Approach for Precipitation Nowcasting," in Advances in Neural Information Processing Systems (NeurIPS), pp. 802–810, 2015.
9. S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.
10. M. T. Ribeiro, S. Singh, and C. Guestrin, "Why Should I Trust You? Explaining the Predictions of Any Classifier," in Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1135–1144, 2016.
11. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," Journal of Information Security and Applications, vol. 50, 2020.
12. G. Thamilarasu and S. Chawla, "Towards Deep-Learning-Driven Intrusion Detection Systems on the Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2476–2490, 2020.
13. Y. Wu et al., "A Comprehensive Survey of Deep Learning-Based Intrusion Detection Systems," Computer Networks, vol. 205, 2022.