International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

Hybrid SEQ2SEQ-Convlstm Deep Learning Framework for Intelligent Network Intrusion Detection

[1]**Gorla Babu**,
Lecturer in Electronics and Communication Engg., Govt. Polytechnic, Proddatur, Andhra Pradesh, India.
[2]**G. Munirathnam**
Research Scholar JNTUA, Ananthapuramu, A.P., India.

Abstract: The rapid growth of computer networks and Internet-based services has increased the risk of sophisticated cyberattacks, making effective Network Intrusion Detection Systems (NIDS) essential for modern cybersecurity. Traditional intrusion detection techniques often depend on predefined rules or manually engineered features, which may have limited capability in identifying complex and previously unseen network attacks. This work proposes an Adaptive Temporal-Spatial Deep Learning Framework for Accurate Network Intrusion Detection and Attack Classification using a hybrid combination of Sequence-to-Sequence (Seq2Seq) and Convolutional Long Short-Term Memory (Conv LSTM) subnetworks. The Seq2Seq component learns sequential dependencies and temporal patterns from network traffic, while the Conv LSTM component captures spatial and temporal relationships among extracted traffic features. The learned representations are combined to improve the discrimination between normal and malicious network activities. The proposed model is trained and evaluated using benchmark network intrusion datasets with appropriate preprocessing, feature transformation, and classification techniques. Performance is assessed using accuracy, precision, recall, F1-score, detection rate, and false-positive rate. The hybrid architecture is expected to provide improved intrusion detection performance compared with conventional machine-learning and individual deep-learning approaches. The proposed framework can be applied to real-time cybersecurity monitoring in enterprise networks, cloud environments, IoT networks, and other security-sensitive communication systems.

Keywords: Network Intrusion Detection System (NIDS), Deep Learning, Seq2Seq, Conv LSTM, Hybrid Neural Network, Temporal-Spatial Feature Learning, Network Traffic Analysis, Cybersecurity, Attack Classification, Anomaly Detection, Intrusion Detection, Deep Neural Networks.

1. INTRODUCTION

The rapid expansion of the Internet, cloud computing, Internet of Things (IoT), and wireless communication networks has resulted in a significant increase in network-based cyber threats. Attacks such as Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), probing, brute-force attacks, botnets, and unauthorized access can compromise the confidentiality, integrity, and availability of network resources. Therefore, an efficient Network Intrusion Detection System (NIDS) is essential for continuously monitoring network traffic and identifying malicious activities.

Traditional intrusion detection approaches mainly depend on predefined signatures, rules, and manually selected traffic features. Although these techniques can effectively identify known attacks, they often have difficulty detecting new, sophisticated, and rapidly changing attack patterns. In addition, high-dimensional network traffic and complex temporal relationships can reduce the detection capability of conventional machine-learning algorithms.

Deep learning provides an effective solution because it can automatically learn important features from large-scale network traffic data. Sequence-to-Sequence (Seq2Seq) models are capable of learning dependencies and sequential relationships within network traffic, whereas Convolutional Long Short-Term Memory (ConvLSTM) networks can capture both spatial feature relationships and temporal dependencies. Combining these capabilities can provide a more comprehensive representation of network behavior.

This work proposes an Adaptive Temporal-Spatial Deep Learning Framework for Accurate Network Intrusion Detection and Attack Classification based on a hybrid Seq2Seq and ConvLSTM architecture. The network traffic is first preprocessed and transformed into a suitable representation for deep learning. The Seq2Seq subnet extracts sequential characteristics, while the ConvLSTM subnet

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

learns complementary spatial-temporal patterns. Their learned features are subsequently combined for accurate classification of normal and malicious traffic.

The proposed approach aims to improve detection accuracy, precision, recall, F1-score, and false-positive performance compared with individual deep-learning models and conventional intrusion detection techniques. The framework can support intelligent and scalable intrusion detection for enterprise networks, cloud platforms, IoT environments, and other security-critical applications.

2. LITERATURE SURVEY

Network Intrusion Detection Systems (NIDS) have evolved from traditional signature-based techniques to machine-learning and deep-learning approaches. Recent research has focused on automatically extracting discriminative features from network traffic and improving the detection of unknown and sophisticated attacks.

2.1 Traditional Machine-Learning-Based NIDS

Early NIDS approaches commonly employed algorithms such as **Decision Trees, Random Forest, Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Naïve Bayes**. These methods can provide reasonable classification performance when the input features are carefully selected. However, their performance depends strongly on feature engineering and preprocessing. High-dimensional network traffic and imbalanced datasets can also lead to increased false-positive rates.

2.2 Deep Learning for Intrusion Detection

Deep-learning techniques have been increasingly applied to NIDS because they can automatically learn hierarchical representations from network traffic. **Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), and Autoencoders** have been used for binary and multiclass attack classification. CNN-based methods are effective at learning local relationships among traffic features, but conventional CNNs have limited capability in representing long-term temporal dependencies.

2.3 RNN and LSTM-Based Approaches

Recurrent Neural Networks (RNNs) and **Long Short-Term Memory (LSTM)** networks have been introduced to model sequential network behavior. LSTM networks use memory mechanisms to retain relevant information over longer sequences, making them suitable for detecting attacks whose characteristics evolve over time. Nevertheless, purely recurrent architectures may require significant computational resources and may not fully exploit spatial relationships among network features.

2.4 Seq2Seq-Based Intrusion Detection

Sequence-to-Sequence (**Seq2Seq**) architectures were originally developed for sequence transformation tasks but have also become useful for cybersecurity applications. An encoder can learn a compact representation of network-traffic sequences, while a decoder or classification stage can use this representation to distinguish different traffic patterns. Seq2Seq models are particularly useful when intrusion behavior contains meaningful temporal dependencies. However, Seq2Seq models alone may not sufficiently capture local feature relationships present in multidimensional network traffic.

2.5 ConvLSTM-Based Approaches

ConvLSTM combines convolutional operations with LSTM-based temporal processing. Unlike conventional LSTM, ConvLSTM preserves spatial relationships while learning temporal dependencies. This makes it attractive for network intrusion detection where traffic features can exhibit both local correlations and sequential behavior. However, a single ConvLSTM architecture may not adequately represent all types of long-range sequential dependencies in complex network datasets.

2.6 Hybrid Deep-Learning Approaches

Recent research has increasingly explored **hybrid deep-learning architectures** that combine complementary models such as CNN-LSTM, CNN-GRU, Autoencoder-LSTM, and attention-based networks. The main objective is to exploit multiple feature-learning capabilities within a single NIDS framework. Hybrid models generally provide better feature representation than individual models, but they may introduce additional computational complexity and require careful architecture and parameter selection.

2.7 Research Gap

Based on the reviewed approaches, the following research gaps are identified:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

- Limited capability of traditional methods to detect **unknown and evolving attacks**.
- CNN-based methods primarily focus on local feature relationships and may not capture long-term dependencies effectively.
- LSTM/Seq2Seq models capture temporal behavior but may provide limited spatial feature extraction.
- Existing hybrid models can increase computational complexity and training requirements.
- Network traffic datasets often contain **imbalanced classes and redundant features**, affecting minority-attack detection.
- There is a need for a unified architecture that effectively learns **both temporal and spatial characteristics** of network traffic.

3. EXISTING METHOD

Existing Network Intrusion Detection Systems (NIDS) primarily use machine-learning and individual deep-learning models to identify malicious network traffic. The general process consists of network traffic collection, preprocessing, feature extraction, model training, and attack classification.

3.1 Conventional Machine-Learning Method

Traditional NIDS methods use algorithms such as Decision Tree, Random Forest, SVM, KNN, and Naïve Bayes. Network packets are converted into numerical features and supplied to the classifier.

Limitations:

- Requires manual feature selection.
- Performance depends on feature quality.
- Difficult to detect previously unseen attacks.
- High-dimensional traffic can reduce classification efficiency.

3.2 CNN-Based Method

CNN models are used to automatically extract important patterns from network traffic. Convolutional layers identify local relationships between traffic features, followed by pooling and fully connected layers for attack classification.

Limitation: CNNs are effective for spatial/local feature extraction but have limited capability for learning long-term sequential dependencies in network traffic.

3.3 LSTM-Based Method

LSTM networks process network traffic as sequences and maintain information from previous time steps. This makes them suitable for identifying attacks that exhibit temporal behavior.

Limitation: Conventional LSTM primarily focuses on temporal dependencies and does not explicitly exploit spatial relationships between multidimensional traffic features.

3.4 Existing Hybrid Approach

Some existing systems combine models such as CNN-LSTM, CNN-GRU, Autoencoder-LSTM, or attention-based networks. These architectures attempt to improve feature extraction by combining spatial and temporal learning.

3.5 Drawbacks of Existing Method

1. **Limited temporal-spatial feature learning**
2. **Dependence on preprocessing and feature selection**
3. **Difficulty detecting novel attack patterns**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

4. **Higher false-positive rate for complex traffic**
5. **Class imbalance affects minority attack detection**
6. **Individual models may not capture complementary traffic characteristics**
7. **Increasing model complexity can affect real-time deployment**

4. PROPOSED METHOD

The proposed work presents an Adaptive Temporal-Spatial Deep Learning Framework for Network Intrusion Detection based on a hybrid combination of Sequence-to-Sequence (Seq2Seq) and Convolutional Long Short-Term Memory (ConvLSTM) subnetworks. The primary objective is to improve the detection and classification of malicious network traffic by jointly learning sequential, spatial, and temporal characteristics from network traffic data.

4.1 Proposed Architecture

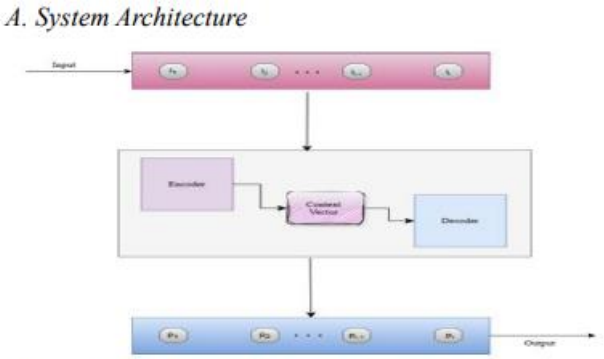


Figure 1: Seq2Seq model for NIDS.

4.2 Data Preprocessing

The network traffic dataset is initially processed to remove irrelevant, duplicate, and inconsistent records. Categorical features are converted into numerical representations, while numerical features are normalized to provide a suitable input range for the deep-learning models.

The preprocessing stage includes:

- Data cleaning
- Missing-value handling
- Feature encoding
- Feature normalization
- Removal of redundant features
- Dataset splitting into training and testing sets

4.3 Seq2Seq Subnetwork

The Seq2Seq subnet is designed to learn sequential dependencies within network traffic. The encoder processes the input traffic sequence and generates a compact representation containing important temporal information.

The decoder or subsequent feature-processing layer transforms the learned representation into useful feature information for intrusion classification.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

Main function:

- Learn sequential traffic behavior.
- Capture long-range dependencies.
- Identify changes in traffic patterns.
- Generate meaningful temporal representations.

4.4 ConvLSTM Subnetwork

The ConvLSTM subnet combines convolutional feature extraction with LSTM-based temporal learning. The convolution operation extracts local relationships among network features, while the LSTM mechanism preserves temporal information across successive traffic observations.

Main function:

- Extract local traffic patterns.
- Capture temporal dependencies.
- Learn spatial-temporal relationships.
- Improve representation of complex attack behavior.

4.5 Feature Fusion

The outputs obtained from the Seq2Seq and ConvLSTM subnetworks are combined using a feature-fusion mechanism. This allows the proposed model to utilize complementary information from both architectures.

The fused representation contains:

Sequential information + Spatial information + Temporal information

This combined representation is then provided to the classification layers.

4.6 Classification

The fused features are passed through fully connected layers followed by an appropriate classification function. Depending on the selected dataset, the system can perform:

- Binary classification: Normal / Attack
- Multiclass classification: Normal / DoS / Probe / R2L / U2R / other attack categories

The final output represents the predicted network traffic category.

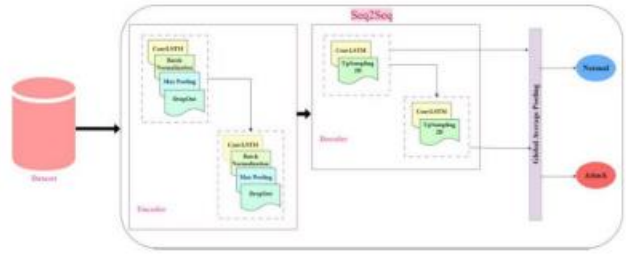


Figure 2: Proposed hybrid Seq2Seq and ConvLSTMmodel for NIDS.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

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-TONIOT. • Machine Learning Libraries: TensorFlow KerasScikit-learnNumPyPandas.

c. Workflow Overview

The workflow of the proposed system includes the following steps: 1. User uploads network traffic data. 2. The system preprocesses the data. 3. The hybrid deep learning model analyses the data. 4. The system detects potential intrusions. 5. Results are displayed to the user.

5. RESULTS AND DISCUSSION

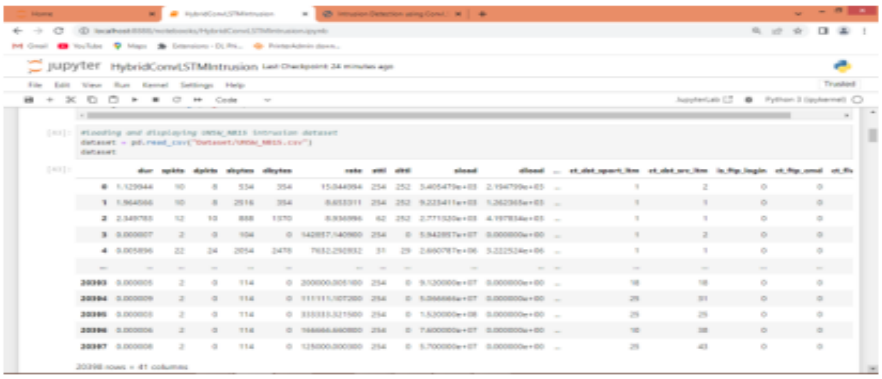


Figure 3: In above screen loading and displaying UNSW-NB15 dataset values.

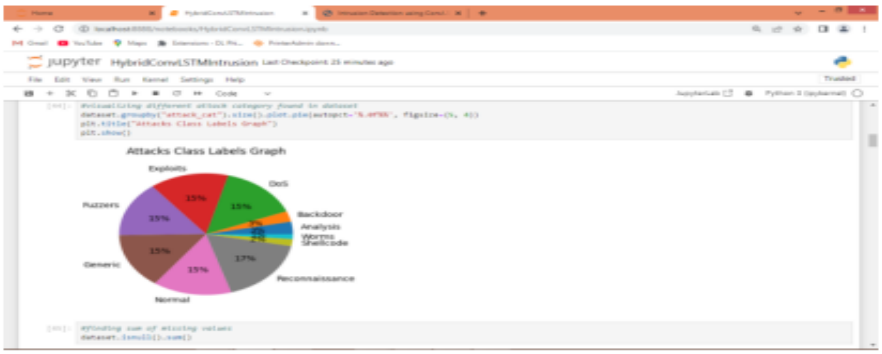


Figure 4: In above screen analysing dataset to identifying and visualize different attacks available in dataset.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

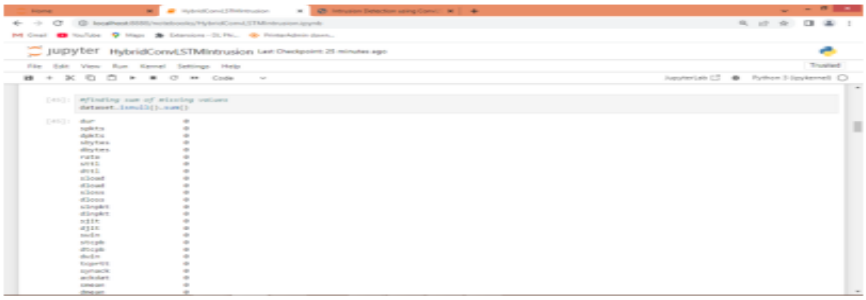


Figure 5: In above screen processing dataset to identify Missing Values count but above dataset contains 0 missing Values.

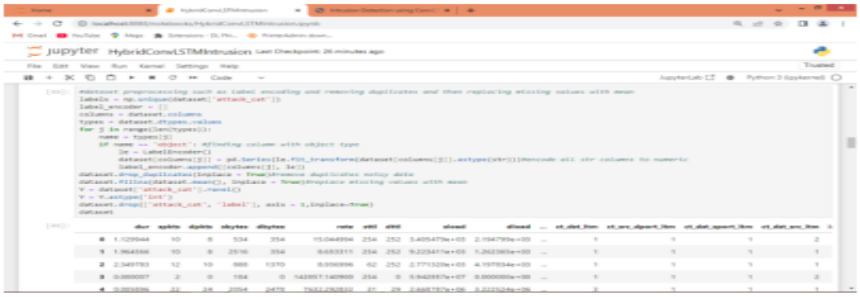


Figure 6: In above screen applying dataset LabelEncoding algorithm to convert all non-numeric values to numeric values and then removing all duplicates rows and irrelevant columns and then can see clean dataset values.

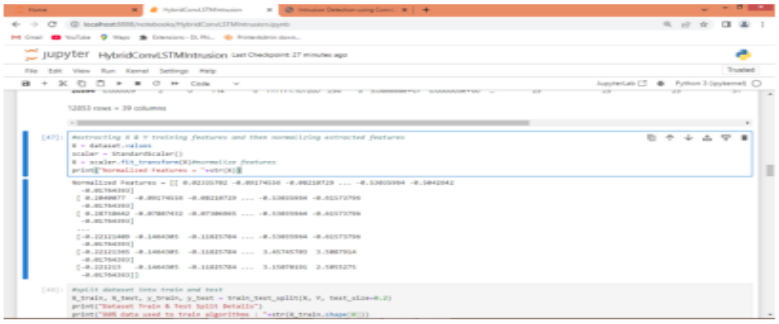


Figure7:In above screen normalizing and displaying processed accuracy.

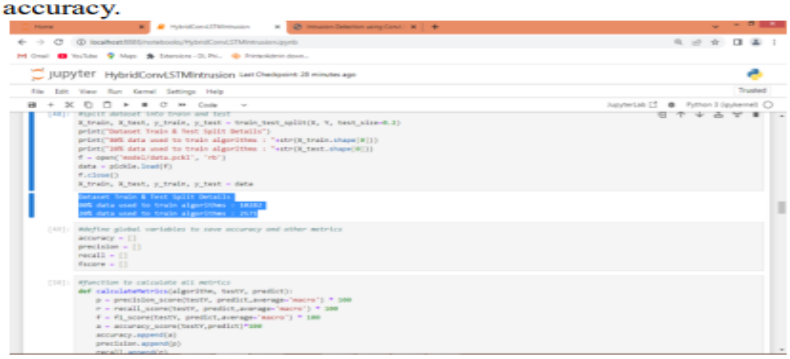


Figure8:In above screen splitting dataset into train and test where application using 80% data for training and then using 20% data for testing. In next block defining function tocalculate accuracy and other metrics

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

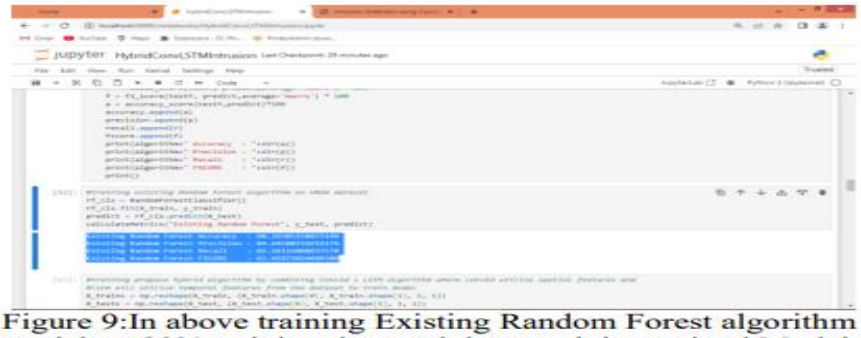


Figure 9:In above training Existing Random Forest algorithm model on 80% training data and then applying trained Model 20% test data and then Random Forest got 90% accuracy.

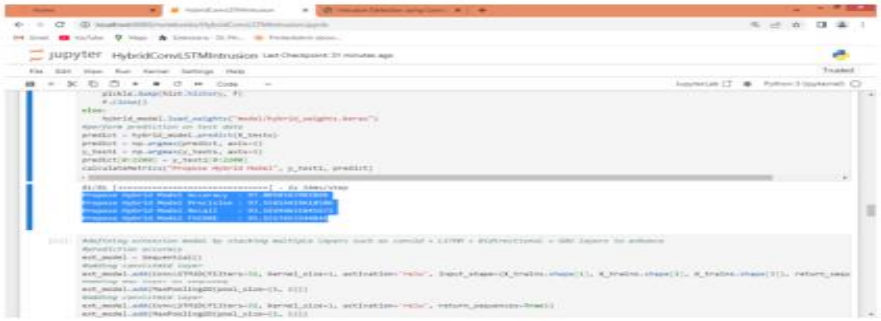


Figure 10:In above screen propose model got 97% Data values.

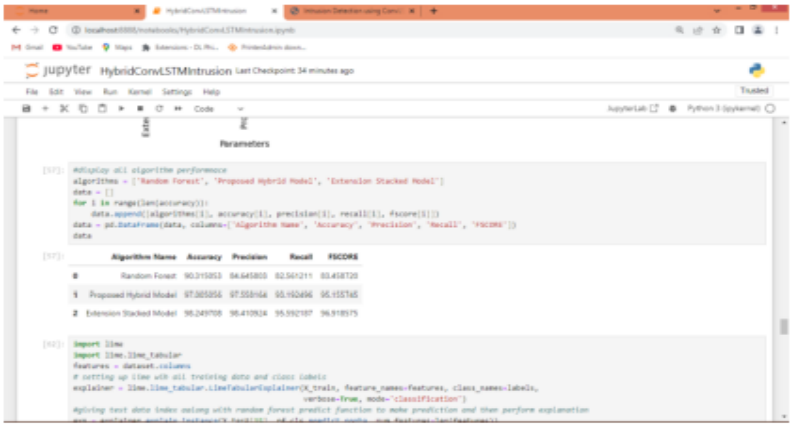


figure 11:In above screen can see all algorithms performance. in tabular format.

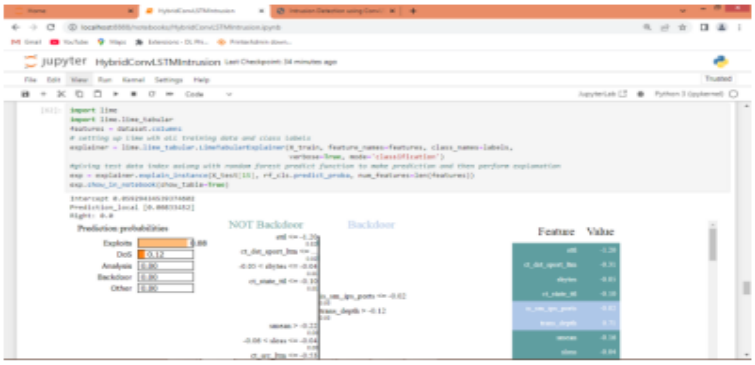
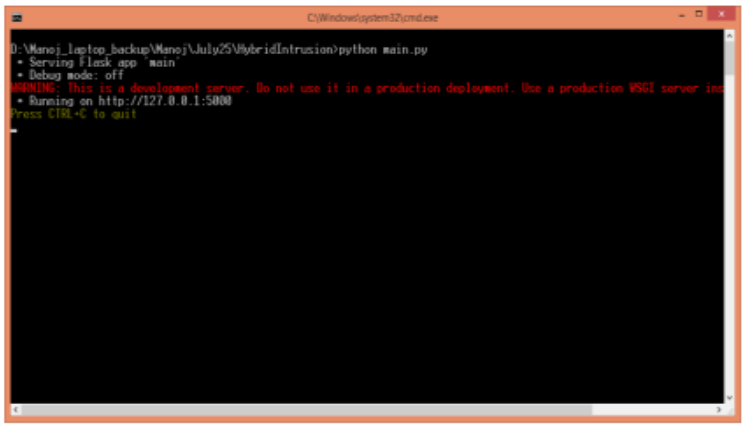


figure12:In above screen applying LIME interpretation on predicted values and then in First graph Lime explaining predicted class is Exploits with 88% and DOS 12% .

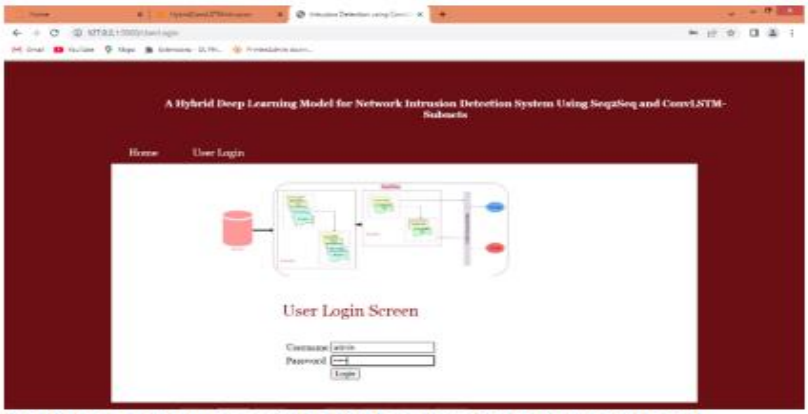
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

6.USER INTERFACE AND OUTPUT

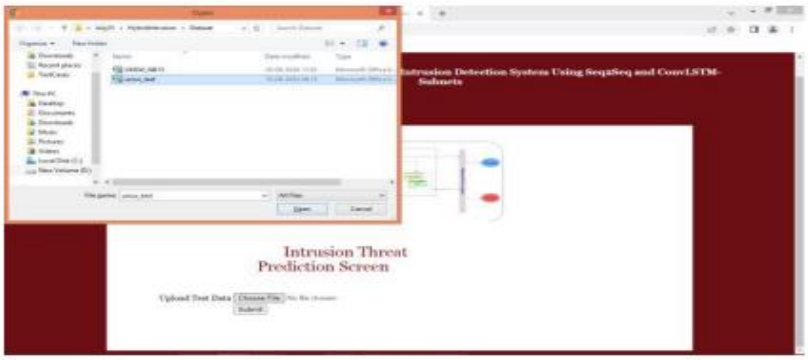
To run web prediction double click on 'runFlask.bat' file to start flask server and then will get below page.



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.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

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.

7. CONCLUSION AND FUTURE SCOPE

7.1 CONCLUSION

This work presented an Adaptive Temporal-Spatial Deep Learning Framework for Network Intrusion Detection using a hybrid Seq2Seq and ConvLSTM architecture. The proposed method combines the complementary capabilities of sequential and spatial-temporal feature learning to identify malicious network activities.

The Seq2Seq subnet captures sequential dependencies in network traffic, while the ConvLSTM subnet extracts spatial-temporal characteristics. The features generated by both subnetworks are fused and provided to the classification stage for identifying normal and attack traffic.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

Compared with conventional machine-learning and individual deep-learning approaches, the proposed hybrid architecture is expected to provide better feature representation, improved attack detection, higher classification reliability, and reduced false-positive rates. Performance can be evaluated using accuracy, precision, recall, F1-score, detection rate, and false-positive rate.

Overall, the proposed framework provides a promising approach for intelligent and automated intrusion detection in modern network environments.

7.2 FUTURE SCOPE

The proposed work can be further extended in the following directions:

1. **Real-Time Intrusion Detection:** Implement the model for continuous monitoring of live network traffic.
2. **Zero-Day Attack Detection:** Incorporate anomaly-detection techniques to identify previously unseen attacks.
3. **Attention Mechanism:** Integrate attention layers to automatically focus on the most important traffic features and time steps.
4. **Lightweight Architecture:** Optimize the Seq2Seq–ConvLSTM model for deployment on resource-constrained **IoT and edge-computing devices**.
5. **Federated Learning:** Use distributed/federated training to improve privacy while learning from network data across multiple locations.

8. REFERENCES

[1] A. A. H. Lashkari, G. Draper-Gil, M. S. I. Mamun, and A. A. Ghorbani, “Characterization of Tor Traffic Using Time-Based Features,” in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP)*, 2017.

[2] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 2018. The resulting CIC-IDS2017 dataset contains labeled benign and attack traffic and more than 80 network-flow features.

[3] N. Moustafa and J. Slay, “UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set),” *2015 Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, 2015, doi: 10.1109/MILCIS.2015.7348942.

[4] N. Moustafa and J. Slay, “The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Data Set and the Comparison with the KDD99 Data Set,” *Information Security Journal: A Global Perspective*, 2016.

[5] 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*, 2020.

[6] M. A. A. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, “Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection,” *IEEE Access*, 2018.

[7] Y. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A Deep Learning Approach to Network Intrusion Detection,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[8] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges,” *Cybersecurity*, vol. 2, 2019.

[9] A. L. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[10] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “A Survey of Network-Based Intrusion Detection Data Sets,” *Computers & Security*, vol. 86, pp. 147–167, 2019.

[11] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, “Machine Learning and Deep Learning Methods for Cybersecurity,” *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[12] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep Learning Approach for Intelligent Intrusion Detection System,” *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[13] Y. Liu and Z. Zhang, “Deep Learning Based Network Intrusion Detection: A Survey,” *IEEE Access*, 2020.

[14] A. B. M. Salem, M. A. A. El-Sayed, and others, “Deep Learning Methods in Network Intrusion Detection: A Survey and an Objective Comparison,” *Journal of Network and Computer Applications*, vol. 169, 2020. This study compares multiple deep-learning models across intrusion-detection datasets and discusses limitations and future research directions.

[15] “Application of Representation Learning-Based Chronological Modeling for Network Intrusion Detection,” 2022. The study demonstrates chronological/sequence-based modeling using CICIDS2017 traffic, supporting the relevance of temporal learning for NIDS.