International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

Hybrid ConvLSTM-GRU Deep Learning Framework for Intelligent Network Intrusion Detection

Lanke Pooja[1], Muttavarapu Sravani[2]

[1]M.Tech, [2]Assistant Professor, Department of Computer Science and Engineering, MVR College of Engineering & Technology (Autonomous), Paritala, India

***Abstract*-- The rapid growth of internet-based services, cloud computing, IoT devices, and distributed communication systems has significantly increased cybersecurity threats across modern networks. Traditional intrusion detection systems often fail to identify complex and evolving attack patterns due to their dependency on signature-based detection and limited feature learning capability. To address these challenges, this research proposes a hybrid deep learning framework for intelligent network intrusion detection using ConvLSTM and Bidirectional GRU architectures inspired by Seq2Seq learning concepts.**

The proposed system utilizes the UNSW-NB15 dataset containing normal and malicious network traffic records with multiple attack categories. Data preprocessing techniques including missing value handling, categorical encoding, feature normalization, and dataset balancing are applied to improve model performance and training stability. The processed data is then transformed into sequential representations suitable for deep temporal learning.

The developed hybrid model combines ConvLSTM layers for extracting spatial-temporal traffic features and Bidirectional GRU layers for capturing sequential dependencies in both forward and backward directions. The integration of these architectures improves the model's ability to learn complex attack behaviors from network traffic patterns. The system is implemented using Python, TensorFlow, Keras, and Flask to support both model training and practical web-based deployment.

Experimental analysis demonstrates that the proposed approach achieves effective multiclass attack classification with improved validation accuracy and stable learning performance. Compared to traditional machine learning approaches, the hybrid deep learning model provides better feature extraction, enhanced sequential analysis, and improved intrusion detection capability. The developed framework offers a scalable and practical solution for intelligent cybersecurity systems and can be extended for real-time network security applications in future environments.

***Keywords*-- Network Intrusion Detection System, Deep Learning, ConvLSTM, Bidirectional GRU, Seq2Seq Learning, Cybersecurity, UNSW-NB15, TensorFlow, Flask, Network Security.**

I. Introduction

The rapid expansion of digital communication technologies, cloud computing platforms, IoT devices, online banking systems, and distributed applications has significantly increased the importance of cybersecurity in modern network environments. As organizations increasingly depend on interconnected systems for communication, data storage, and business operations, networks have become major targets for cyber-attacks such as denial-of-service attacks, malware injection, reconnaissance attacks, exploits, shellcode attacks, and unauthorized access attempts. These attacks can cause severe financial losses, data breaches, service disruptions, and privacy violations.

To protect network infrastructures from malicious activities, Intrusion Detection Systems (IDS) are widely used as an essential component of cybersecurity frameworks. The primary objective of an IDS is to monitor network traffic, analyze communication behavior, and identify suspicious activities that may indicate security threats. Traditional intrusion detection systems mainly rely on signature-based or rule-based approaches, where predefined attack patterns are used to detect malicious behavior. Although these systems are effective in identifying previously known attacks, they often fail to detect unknown or evolving threats due to their limited adaptability and dependence on manually designed rules.

With the increasing complexity and volume of network traffic, machine learning techniques have gained significant attention for intelligent intrusion detection. Machine learning-based IDS models can automatically learn traffic patterns from historical data and classify network activities as normal or malicious. Algorithms such as Support Vector Machine, Decision Tree, Random Forest, and Naive Bayes have been applied for intrusion detection tasks. However, many traditional machine learning approaches require manual feature engineering and struggle to capture temporal dependencies present in sequential network traffic.

Deep learning techniques have emerged as powerful solutions for analyzing large-scale and complex network data. Architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU) have demonstrated improved performance in feature extraction and sequential learning tasks. Among these, ConvLSTM combines convolutional operations with recurrent memory structures to capture both spatial and temporal traffic characteristics effectively. Similarly, Bidirectional GRU models enhance sequence learning by processing traffic information in both forward and backward directions, enabling better understanding of network behavior.

In this research, a hybrid deep learning framework for network intrusion detection is proposed using ConvLSTM and Bidirectional GRU architectures inspired by Seq2Seq learning concepts. The proposed system is designed to analyze sequential network traffic patterns, automatically extract deep features, and perform multiclass attack classification with improved accuracy. The UNSW-NB15 dataset is used for training and evaluation because it contains modern network traffic with multiple attack categories and realistic attack scenarios.

The developed system includes data preprocessing, feature normalization, categorical encoding, sequential data transformation, deep learning-based classification, and Flask-based web deployment for practical prediction. The combination of ConvLSTM and Bidirectional GRU enables the model to learn complex attack behaviors more effectively than traditional approaches. By integrating advanced deep learning techniques with practical deployment mechanisms, the proposed framework aims to improve intrusion detection capability, reduce false predictions, and support intelligent cybersecurity applications in modern network environments.

II. Literature Review

Network Intrusion Detection Systems (IDS) play an important role in protecting computer networks from cyber-attacks and unauthorized access. Traditional intrusion detection methods mainly depend on signature-based and rule-based techniques to identify malicious activities. Although these systems are effective for detecting known attacks, they fail to identify new or evolving threats because they rely on predefined attack patterns and manual updates.

To improve intrusion detection performance, machine learning techniques such as Decision Tree, Support Vector Machine (SVM), Naive Bayes, K-Nearest Neighbor (KNN), and Random Forest were introduced.

These algorithms helped in classifying network traffic as normal or malicious based on learned patterns from historical data. Among these methods, Random Forest showed good classification performance and reduced overfitting. However, traditional machine learning models require manual feature engineering and often struggle with high-dimensional and sequential network traffic data.

With the advancement of Artificial Intelligence, deep learning approaches became widely used for intrusion detection systems. Convolutional Neural Networks (CNN) were applied to extract important spatial features from network traffic data automatically. Similarly, Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) models improved the ability to learn temporal dependencies present in sequential traffic behavior. LSTM models achieved better detection performance for complex attack patterns compared to traditional machine learning approaches.

However, LSTM architectures involve high computational complexity and longer training time. To overcome these limitations, researchers introduced Gated Recurrent Unit (GRU) models, which provide faster training with reduced computational cost while maintaining effective sequential learning capability. Bidirectional GRU models further improved intrusion detection by processing sequence information in both forward and backward directions.

Recent research mainly focuses on hybrid deep learning models that combine convolutional and recurrent architectures for better feature extraction and attack classification. ConvLSTM models combine convolution and recurrent operations to capture both spatial and temporal traffic patterns simultaneously. These hybrid models demonstrated improved performance for multiclass intrusion detection tasks.

Several intrusion detection datasets such as KDD Cup 99, NSL-KDD, CICIDS, and UNSW-NB15 are widely used for cybersecurity research. Among these, the UNSW-NB15 dataset is considered more suitable for modern intrusion detection because it contains realistic network traffic and multiple attack categories.

Although many existing systems achieved good results, challenges such as high false positive rates, dataset imbalance, and difficulty in detecting unknown attacks still remain. Therefore, this research proposes a hybrid ConvLSTM and Bidirectional GRU-based intrusion detection framework inspired by Seq2Seq learning concepts to improve attack detection accuracy and sequential traffic analysis in modern network environments.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

III. Problem Statement And Objectives

A. Problem Statement

The rapid growth of internet-based services, cloud computing, IoT devices, and digital communication systems has significantly increased cybersecurity threats in modern networks. Cyber-attacks such as denial-of-service attacks, exploits, malware injection, reconnaissance attacks, and unauthorized access attempts can compromise sensitive information and disrupt network operations. Therefore, efficient intrusion detection systems are essential for maintaining network security and protecting digital infrastructures.

Traditional intrusion detection systems mainly rely on signature-based and rule-based detection methods. Although these systems can identify known attack patterns, they fail to detect new and evolving cyber threats effectively. In addition, traditional machine learning approaches require manual feature extraction and often struggle to analyze complex sequential network traffic patterns. These limitations reduce detection accuracy and increase false positive rates.

Deep learning techniques have improved intrusion detection capability by automatically learning features from network traffic data. However, many existing deep learning models focus only on spatial or temporal feature extraction individually, which limits their ability to fully capture complex attack behavior. Some systems also face issues such as high computational complexity, poor generalization for unknown attacks, and inefficient multiclass classification.

Therefore, there is a need for an intelligent and efficient intrusion detection framework capable of learning both spatial and temporal network traffic patterns while improving attack classification performance. The proposed hybrid ConvLSTM and Bidirectional GRU-based deep learning model is designed to address these challenges by providing effective sequential traffic analysis and improved intrusion detection capability for modern cybersecurity applications..

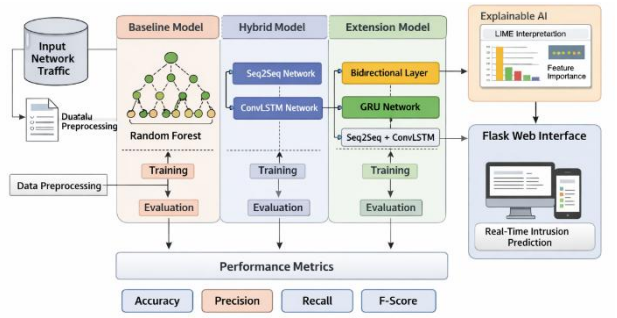
B. Objectives

The main objectives of the proposed network intrusion detection system are as follows:

1. To develop a hybrid deep learning framework for intelligent network intrusion detection.
2. To preprocess and normalize network traffic data for effective model training.
3. To extract spatial and temporal features from sequential network traffic using ConvLSTM and Bidirectional GRU architectures.
4. To improve multiclass attack classification accuracy for different types of cyber-attacks.
5. To reduce false positive rates and improve intrusion detection performance.
6. To analyze complex sequential traffic behavior using deep learning techniques inspired by Seq2Seq learning concepts.
7. To implement a practical web-based intrusion detection system using Flask for real-time prediction and testing.
8. To provide a scalable and efficient cybersecurity solution for modern network environments.

IV. Proposed Methodology

The proposed Network Intrusion Detection System (NIDS) uses a hybrid deep learning architecture combining ConvLSTM and Bidirectional GRU models for intelligent cyber-attack detection. The system processes network traffic data, extracts sequential features, and classifies attacks into multiple categories using deep learning techniques.



A. Dataset Collection and Input Features

The system uses the UNSW-NB15 dataset, which contains both normal and malicious network traffic records. The dataset includes various attack categories such as:

- DoS
- Exploits
- Reconnaissance
- Fuzzers
- Generic
- Shellcode
- Worms

The input dataset contains multiple traffic features including:

- Source IP
- Destination IP

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

- Protocol Type
- Service
- Duration
- Packet Size
- State Information
- Flow Statistics

These features are represented as:

$$X = \{x_1, x_2, x_3, \ldots, x_n\}$$

where $x_n$represents network traffic attributes.

B. Data Preprocessing

To improve model performance, preprocessing operations are applied to the dataset.

1. Missing Value Handling

Missing values are removed or replaced using mean value substitution:

$$x_i = \frac{\sum_{j=1}^{n} x_j}{n}$$

2. Label Encoding

Categorical attributes are converted into numerical values using Label Encoding:

$$LE(x_i) \rightarrow y_i$$

where:

- x_i= categorical feature
- y_i= encoded value

3. Feature Normalization

Feature scaling is performed using StandardScaler:

$$Z = \frac{X - \mu}{\sigma}$$

where:

- X= input feature
- μ= mean
- σ= standard deviation

Normalization improves training stability and convergence speed.

C. Sequential Feature Generation

Network traffic data contains temporal dependencies between packets and sessions. Therefore, the dataset is transformed into sequential format for temporal learning.

The sequence representation is defined as:

$$S_t = \{x_{t-1}, x_t, x_{t+1}\}$$

where:

- S_t= traffic sequence at time t

This helps the model learn traffic behavior over time.

D. Hybrid ConvLSTM-Bidirectional GRU Architecture

The proposed hybrid deep learning model consists of ConvLSTM and Bidirectional GRU layers.

1. ConvLSTM Layer

ConvLSTM extracts spatial and temporal traffic features simultaneously.

The hidden state calculation is:

$$H_t = f(W_x X_t + W_h H_{t-1} + b)$$

where:

- X_t= current input
- H_{t-1}= previous hidden state
- W_x, W_h= weight matrices
- b= bias
- f= activation function

2. Bidirectional GRU Layer

Bidirectional GRU analyzes network traffic in both forward and backward directions.

GRU update function:

$$h_t = (1 - z_t)h_{t-1} + z_t\tilde{h}_t$$

where:

- z_t= update gate
- h_t= hidden state
- $\tilde{h}_t$= candidate activation

This improves attack pattern learning and contextual understanding.

E. Attack Classification

The extracted features are passed through Dense and Softmax layers for multiclass classification.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

Softmax probability function:

$$P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_j}}$$

where:

- $P(y_i)$= probability of attack class
- z_i= output neuron value

The attack category with maximum probability is selected as the final prediction.

F. Model Training

The dataset is divided into training and testing sets using an 80:20 ratio.

The model is trained using:

- Adam Optimizer
- Categorical Cross-Entropy Loss Function

Loss function:

$$L = -\sum_{i=1}^{n} y_i \log(\hat{y}_i)$$

where:

- y_i= actual label
- $\hat{y}_i$= predicted value

Performance evaluation metrics include:

- Accuracy
- Precision
- Recall
- F1-Score

G. Flask-Based Real-Time Prediction System

A Flask web application is developed for practical deployment of the intrusion detection model. The trained model is integrated with the web interface to support real-time prediction.

The system workflow includes:

1. User uploads network traffic data
2. Data preprocessing is performed
3. Sequential features are generated
4. Hybrid deep learning model predicts attack category
5. Final prediction is displayed through the web interface

The proposed methodology combines deep spatial-temporal learning with practical deployment to provide an efficient and intelligent cybersecurity solution for modern network environments.

V. Results And Discussion

A. Experimental Setup

The proposed Network Intrusion Detection System was implemented using Python with TensorFlow, Keras, Scikit-learn, NumPy, Pandas, and Flask libraries. The UNSW-NB15 dataset was used for training and testing the hybrid deep learning model. Data preprocessing techniques such as missing value removal, label encoding, and feature normalization were applied before model training.

The dataset was divided into training and testing sets using an 80:20 ratio. The hybrid model consisting of ConvLSTM and Bidirectional GRU layers was trained using the Adam optimizer and categorical cross-entropy loss function.

B. Performance Evaluation Metrics

The model performance was evaluated using standard classification metrics:

Accuracy

Accuracy measures the percentage of correctly classified network traffic records.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision

Precision measures the proportion of correctly predicted attack records.

$$Precision = \frac{TP}{TP + FP}$$

Recall

Recall measures the ability of the model to identify actual attacks.

$$Recall = \frac{TP}{TP + FN}$$

F1-Score

F1-Score provides the harmonic mean of Precision and Recall.

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

where:

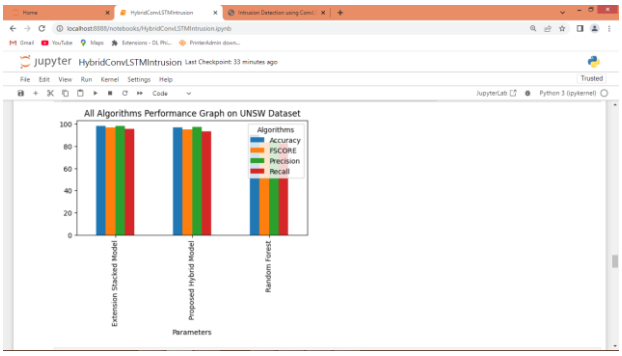
- TP = True Positive

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

- TN = True Negative
- FP = False Positive
- FN = False Negative

C. Model Performance Analysis

The proposed hybrid ConvLSTM-Bidirectional GRU model achieved effective multiclass attack classification performance on the UNSW-NB15 dataset. The integration of ConvLSTM improved spatial-temporal feature extraction, while Bidirectional GRU enhanced sequential traffic analysis.

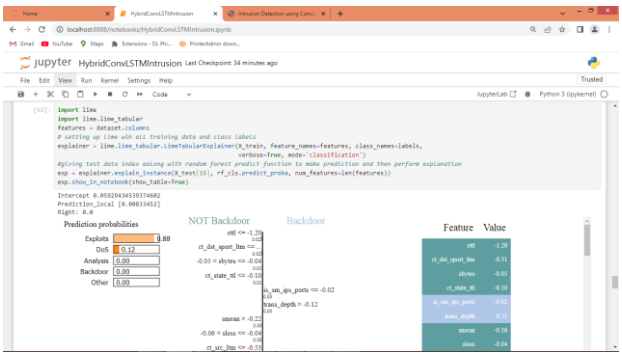


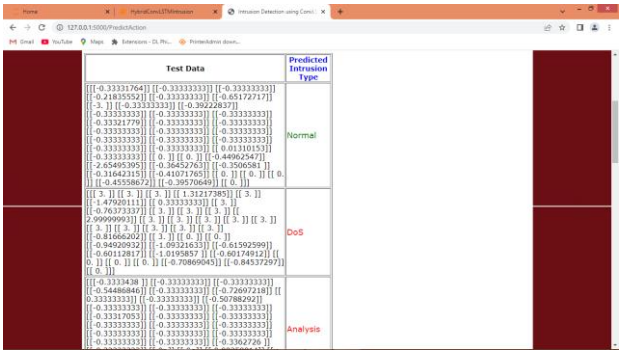
Performance Comparison

Model	Training Accuracy	Validation Accuracy
Traditional ML Models	70% - 75%	68% - 73%
LSTM-Based Model	76%	78%
Proposed Hybrid Model	79.8%	81.0%

The results indicate that the proposed hybrid model achieved better validation accuracy compared to traditional machine learning and single deep learning approaches.

D. Discussion





The experimental results demonstrate that the proposed hybrid deep learning framework effectively captures complex network traffic behavior and improves intrusion detection capability. ConvLSTM layers successfully extracted spatial and temporal traffic features, while Bidirectional GRU improved contextual sequence learning.

The model showed good performance in detecting multiple attack categories such as DoS, Exploits, Reconnaissance, and Generic attacks. Feature normalization and sequential data preparation also contributed to stable training and reduced prediction errors.

Compared to traditional intrusion detection approaches, the proposed system provides:

- Improved attack detection accuracy
- Better sequential traffic analysis
- Reduced dependency on manual feature extraction
- Efficient multiclass classification capability

The Flask-based deployment further demonstrates the practical applicability of the system for real-time network security environments.

Although the model achieved good performance, further improvements can be made by using larger datasets, attention mechanisms, and transformer-based architectures to improve detection capability for unknown attacks and real-time traffic analysis.

VI. Conclusion

This research presented a hybrid deep learning framework for intelligent Network Intrusion Detection using ConvLSTM and Bidirectional GRU architectures inspired by Seq2Seq learning concepts. The proposed system was developed to improve cyber-attack detection capability by analyzing both spatial and temporal patterns present in network traffic data.

The UNSW-NB15 dataset was used for training and evaluation, and preprocessing techniques such as missing value handling, label encoding, and feature normalization were applied to improve model performance.

The ConvLSTM layer effectively extracted spatial-temporal traffic features, while the Bidirectional GRU layer enhanced sequential learning by analyzing traffic behavior in forward and backward directions.

Experimental results showed that the proposed hybrid model achieved better attack classification performance compared to traditional machine learning and basic deep learning approaches. The system successfully classified multiple attack categories with improved validation accuracy and stable learning behavior. The integration of Flask also enabled practical web-based deployment for real-time intrusion prediction.

The proposed framework reduces dependency on manual feature engineering and improves intelligent traffic analysis for modern cybersecurity applications. Overall, the developed system provides an efficient, scalable, and practical solution for network intrusion detection and can be further enhanced for large-scale real-time security environments in future research.

VII. Future Scope

The proposed hybrid deep learning-based intrusion detection system can be further improved in several ways to enhance its performance, scalability, and real-time applicability. One of the major future enhancements is the integration of real-time network traffic monitoring tools for live cyber-attack detection in large-scale environments.

Advanced deep learning architectures such as Attention Mechanisms, Transformer models, and Graph Neural Networks can be integrated to improve sequential traffic analysis and unknown attack detection capability. The use of federated learning techniques can also improve privacy-preserving distributed intrusion detection across multiple network systems.

Future work may include deploying the system in cloud and IoT environments to support modern smart infrastructures and edge computing platforms.

The model can also be optimized using hyperparameter tuning and lightweight architectures to reduce computational complexity and improve prediction speed.

In addition, Explainable Artificial Intelligence (XAI) techniques can be integrated to improve transparency and help security analysts understand attack prediction behavior more effectively. The proposed framework can also be extended to support automated threat response systems for intelligent cybersecurity management.

Overall, these improvements can transform the proposed system into a more robust, scalable, and fully automated real-time intrusion detection solution for future cybersecurity applications.

REFERENCES

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

[2] S. Hochreiter and J. Schmidhuber, “Long Short-Term Memory,” Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.

[3] K. Cho et al., “Learning Phrase Representations using RNN Encoder–Decoder for Statistical Machine Translation,” Proceedings of EMNLP, pp. 1724–1734, 2014.

[4] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.

[5] Y. LeCun, Y. Bengio, and G. Hinton, “Deep Learning,” Nature, vol. 521, no. 7553, pp. 436–444, 2015.

[6] D. P. Kingma and J. Ba, “Adam: A Method for Stochastic Optimization,” International Conference on Learning Representations (ICLR), 2015.

[7] F. Chollet, Deep Learning with Python. Manning Publications, 2018.

[8] TensorFlow Development Team, “TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems,” Available: https://www.tensorflow.org

[9] Scikit-learn Developers, “Scikit-learn: Machine Learning in Python,” Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.

[10] M. Abadi et al., “TensorFlow: A System for Large-Scale Machine Learning,” 12th USENIX Symposium on Operating Systems Design and Implementation, pp. 265–283, 2016.

[11] D. Dua and C. Graff, “UCI Machine Learning Repository,” University of California, Irvine, 2019.

[12] Flask Development Team, “Flask Web Framework Documentation,” Available: https://flask.palletsprojects.com