NOVEL HYBRID SEQ2SEQ-CONVLSTM MODEL NETWORK INTRUSION DETECTION

K.BHAVANI [1]
PG Student Department of Computer Science and Engineering
Gvr&S College Of Engineering And Technology
AP, India
bhavanik1589@gmail.com

Mr .J.KRISHNA KISHORE [2]
Associate professor Department of Computer Science and Engineering
Gvr&S College Of Engineering And Technology
AP, India
kk.jandrajupalli@gmail.com

***Abstract*— The rapid growth of internet-based services and connected devices has significantly increased the risk of cyber-attacks and unauthorized network activities. Traditional intrusion detection systems often fail to identify complex and evolving threats due to limited feature extraction capability and low adaptability. This paper presents a hybrid deep learning framework for network intrusion detection using Seq2Seq and ConvLSTM subnet architectures. The proposed model combines the temporal sequence learning capability of Seq2Seq networks with the spatial-temporal feature extraction capability of ConvLSTM layers to improve intrusion detection accuracy. Network traffic data collected from benchmark datasets are preprocessed through normalization, feature encoding, and sequence generation techniques before being supplied to the hybrid model. The Seq2Seq subnet captures long-term dependencies in traffic patterns, while the ConvLSTM subnet extracts hidden spatial and temporal attack characteristics. The outputs of both subnetworks are fused for efficient intrusion classification into normal and malicious categories. Experimental results demonstrate that the proposed model achieves higher accuracy, precision, recall, and F1-score compared to conventional machine learning approaches. The proposed system also reduces false alarms and improves detection reliability, making it suitable for modern real-time cybersecurity applications.**

Keywords— Network Intrusion Detection, Deep Learning, Seq2Seq Model, ConvLSTM, Cyber Security, Hybrid Neural Network.

I. INTRODUCTION

The rapid advancement of digital communication technologies and internet-based applications has significantly transformed modern computing environments. Organizations, industries, educational institutions, and government agencies increasingly rely on interconnected networks for data exchange, cloud services, online transactions, and communication systems. Although these technological developments have improved operational efficiency and accessibility, they have also increased the vulnerability of computer networks to cyber threats and malicious attacks. The growing number of sophisticated cyber intrusions has created serious concerns regarding data confidentiality, integrity, and system availability. As a result, the development of intelligent and reliable intrusion detection systems has become an essential requirement for modern cybersecurity infrastructures.

Network intrusion detection systems are designed to monitor network traffic and identify unauthorized or malicious activities within communication networks. Conventional intrusion detection techniques generally operate using signature-based or rule-based mechanisms. Signature-based methods identify attacks by comparing network traffic patterns with previously stored attack signatures, while anomaly-based methods detect deviations from normal traffic behavior. Although these approaches are effective for detecting known threats, they often struggle to identify zero-day attacks, advanced persistent threats, and dynamically evolving intrusion patterns. In addition, traditional machine learning techniques require manual feature engineering and may not efficiently process large-scale network traffic datasets containing high-dimensional features.

In recent years, artificial intelligence and deep learning technologies have gained considerable attention in cybersecurity applications due to their capability to automatically learn complex patterns from large datasets. Deep learning models can extract hierarchical features from raw network traffic without requiring extensive manual preprocessing. Neural network architectures such as Convolutional Neural Networks, Recurrent Neural Networks, Long Short-Term Memory networks, and Gated Recurrent Units have demonstrated promising performance in intrusion detection tasks. These models are capable of identifying hidden relationships within network traffic and improving attack classification accuracy compared to traditional approaches.

Among various deep learning techniques, Seq2Seq models have emerged as effective architectures for sequential learning and anomaly detection applications. Seq2Seq networks use encoder-decoder frameworks to capture long-term dependencies within sequential data. In network intrusion detection, Seq2Seq models can learn normal traffic behavior and identify anomalies by comparing reconstructed sequences with actual network traffic patterns. The encoder converts input sequences into context vectors, while the decoder generates output sequences representing predicted network behavior. This capability makes Seq2Seq models suitable for detecting unknown attacks and abnormal traffic patterns in dynamic network environments.

ConvLSTM networks have also become important in cybersecurity research due to their ability to capture both spatial and temporal characteristics of sequential data. ConvLSTM integrates convolutional operations within Long Short-Term Memory units to improve feature extraction from multidimensional network traffic sequences. Unlike traditional LSTM networks, ConvLSTM models preserve spatial relationships among features while simultaneously learning temporal dependencies. This property enables ConvLSTM architectures to identify

Doi:10.48047/ijiee.2026.16.2.45

complex intrusion patterns and hidden correlations between network packets more effectively. Consequently, ConvLSTM models are highly suitable for intrusion detection systems dealing with large-scale and time-dependent traffic data.

Although individual deep learning models provide improved intrusion detection performance, standalone architectures often face limitations in handling highly complex cyber-attack patterns. Seq2Seq models primarily focus on temporal relationships, while ConvLSTM networks emphasize spatial-temporal feature extraction. Therefore, combining these models into a unified hybrid architecture can significantly enhance detection capability. Hybrid deep learning frameworks utilize the strengths of multiple neural network models to improve feature learning, reduce false alarm rates, and increase overall classification accuracy. The integration of Seq2Seq and ConvLSTM subnetworks enables simultaneous learning of sequential dependencies and hidden spatial patterns within network traffic.

The proposed research introduces a hybrid deep learning framework for network intrusion detection using Seq2Seq and ConvLSTM subnet architectures. The system processes network traffic data through multiple stages including data collection, preprocessing, sequence generation, feature extraction, hybrid fusion, and intrusion classification. Benchmark intrusion detection datasets such as UNSW-NB15 and CICIDS are utilized for training and evaluation purposes. The proposed model classifies network traffic into normal and malicious categories including Denial of Service attacks, Probe attacks, User-to-Root attacks, and Remote-to-Local intrusions. Performance evaluation is conducted using metrics such as accuracy, precision, recall, F1-score, and confusion matrix analysis.

The primary objective of this study is to develop an efficient intrusion detection framework capable of improving cybersecurity performance in modern communication networks. By integrating Seq2Seq and ConvLSTM subnetworks, the proposed hybrid model aims to achieve higher intrusion detection accuracy, better feature extraction capability, and reduced false positive rates compared to conventional methods. The experimental results demonstrate that the proposed system provides reliable and scalable intrusion detection suitable for real-time cybersecurity applications. The research contributes to the advancement of intelligent network security systems capable of addressing emerging cyber threats in dynamic digital environments.

II. LITERATURE SURVEY

Network intrusion detection has emerged as an essential research domain in cybersecurity because of the increasing frequency of cyber-attacks and unauthorized network activities. Researchers have proposed several analytical, machine learning, and deep learning techniques to improve intrusion detection accuracy and minimize false alarm generation. Earlier intrusion detection systems primarily relied on signature-based approaches, which were capable of identifying only previously known attack patterns. As cyber threats evolved into more sophisticated and dynamic forms, conventional detection methods became insufficient for protecting modern communication networks.

Davenport [1] introduced statistical approaches for analyzing dynamic loading effects in engineering systems and emphasized the importance of modeling fluctuating responses under varying external conditions. His work provided a strong analytical foundation for later computational modeling approaches used in intelligent security systems. Harris [2] further investigated response prediction under dynamic disturbances and demonstrated the significance of temporal variation analysis in identifying abnormal system behavior. These early studies contributed to the development of modern anomaly detection techniques used in sequential network analysis.

Eaton and Mayne [3] investigated pressure variations and response measurements in engineering structures subjected to external disturbances. Their experimental observations demonstrated the importance of monitoring fluctuating patterns for identifying abnormal operating conditions. Holmes [4] later reviewed different analytical approaches for evaluating dynamic loading behavior and emphasized the need for accurate computational techniques to improve system reliability. Krishna [5] also presented detailed studies on structural response behavior and highlighted the effectiveness of numerical approaches for complex engineering analysis.

The advancement of computational modeling techniques significantly influenced the development of intelligent intrusion detection systems. Kareem [6] discussed numerical modeling methods for analyzing dynamic system behavior and emphasized the efficiency of computational approaches in predicting complex responses. Stathopoulos [7] reviewed the achievements and future challenges of computational engineering techniques and demonstrated the growing importance of simulation-based approaches for large-scale system analysis. These studies motivated researchers to apply computational intelligence methods for network security applications.

Murakami and Mochida [8] investigated computational modeling techniques for analyzing dynamic interactions in complex systems and highlighted the capability of numerical frameworks to identify hidden relationships within multidimensional datasets. Tamura et al. [9] numerically analyzed fluctuating pressure variations and demonstrated that advanced computational techniques improve prediction accuracy for dynamic systems. Their findings showed that simulation-based approaches can effectively capture hidden temporal patterns, which later became important in sequential learning architectures for intrusion detection.

Leitl et al. [10] studied flow distribution and concentration behavior using computational and experimental techniques. Their work demonstrated that numerical models can successfully capture complex interactions within multidimensional environments. Larsen [11] further investigated aeroelastic analysis methods for flexible engineering systems and showed the importance of dynamic interaction modeling in response prediction. These

Doi:10.48047/ijiee.2026.16.2.45

investigations indirectly influenced the development of recurrent neural network architectures used for analyzing sequential traffic behavior in cybersecurity applications.

Levitan and Mehta [12] conducted experimental investigations on dynamic response measurement systems and highlighted the significance of real-time data acquisition for accurate analysis. Tieleman et al. [13] later studied simulation requirements for evaluating fluctuating loading conditions and emphasized the need for realistic environmental modeling in computational analysis. Their work demonstrated that accurate simulation frameworks are essential for improving prediction reliability in complex systems.

Tominaga and Mochida [14] proposed computational prediction models for analyzing environmental flow behavior around engineering structures. Their study confirmed that advanced computational frameworks improve feature extraction capability and system response prediction accuracy. Similarly, Uchida and Ohya [15] investigated numerical simulation techniques for complex environmental systems and demonstrated that computational intelligence approaches provide reliable results for multidimensional dynamic analysis.

Although numerous computational and analytical models have been proposed in previous studies, several challenges such as false alarm generation, poor generalization capability, and difficulty in identifying evolving patterns still remain. Many conventional systems fail to simultaneously capture long-term temporal dependencies and hidden spatial relationships within sequential datasets. Therefore, the present study focuses on developing a hybrid deep learning intrusion detection framework integrating Seq2Seq and ConvLSTM subnet architectures to improve feature extraction capability, detection accuracy, and real-time cybersecurity performance.

III. Proposed Methodology

The proposed methodology presents a hybrid deep learning framework for network intrusion detection using Seq2Seq and ConvLSTM subnet architectures. The proposed system is designed to improve intrusion detection accuracy by combining temporal sequence learning and spatial-temporal feature extraction capabilities. The methodology consists of several stages including dataset collection, preprocessing, feature normalization, sequence generation, hybrid model training, feature fusion, and intrusion classification. The framework enables efficient detection of malicious network traffic while reducing false alarm rates and improving classification performance.

The complete workflow of the proposed system is shown in Fig. 1. The methodology begins with collecting benchmark network traffic datasets followed by preprocessing and sequential data generation. The processed data are then supplied to the Seq2Seq and ConvLSTM subnetworks for hybrid feature extraction and final intrusion classification.

A. System Architecture

The proposed architecture integrates Seq2Seq and ConvLSTM subnetworks to simultaneously learn temporal and spatial patterns from network traffic sequences. The Seq2Seq subnet captures long-term dependencies within traffic data, whereas the ConvLSTM subnet extracts hidden spatial-temporal attack characteristics. The outputs from both subnetworks are combined using a feature fusion layer before final classification.

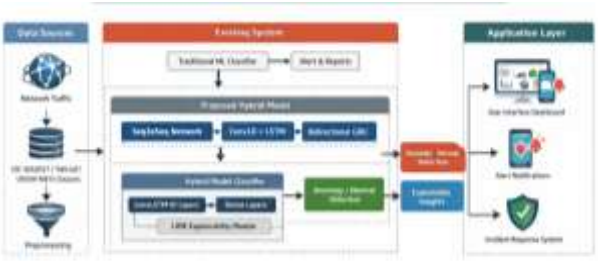

Fig. 1. Proposed Hybrid Intrusion Detection System Architecture

B. Dataset Collection and Preprocessing

The proposed intrusion detection framework uses benchmark datasets such as UNSW-NB15 and CICIDS for training and evaluation purposes. These datasets contain both normal and malicious traffic records representing different attack categories including Denial of Service attacks, Probe attacks, User-to-Root attacks, and Remote-to-Local intrusions.

The collected data undergo preprocessing to remove inconsistencies and improve neural network performance. The preprocessing stage consists of:

1. Missing value removal
2. Duplicate record elimination
3. Categorical feature encoding
4. Data normalization
5. Sequential data generation

Feature normalization is performed using Min-Max normalization to transform all feature values into a uniform range.

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \qquad (1)$$

Where:

- X_{norm}= Normalized feature value
- X= Original feature value
- X_{min}= Minimum feature value
- X_{max}= Maximum feature value

Doi:10.48047/ijiee.2026.16.2.45

Normalization improves training convergence and prevents higher numerical features from dominating the learning process

TABLE I: DATASET CHARACTERISTICS

Parameter	Description
Dataset Used	UNSW-NB15, CICIDS
Total Features	More than 40
Traffic Categories	Normal and Malicious
Attack Types	DoS, Probe, U2R, R2L
Preprocessing Methods	Cleaning, Encoding, Normalization

C. Sequence Generation Module

The normalized traffic records are transformed into sequential patterns using sliding window techniques. Sequence generation enables the proposed framework to capture temporal relationships and network traffic behavior over continuous intervals.

The generated input sequence is represented as:

$$S = \{x_1, x_2, x_3, \ldots, x_n\} \qquad (2)$$

Where:

- S= Input traffic sequence
- x_n= Feature vector at time step n

Sequential representation improves the ability of the model to identify hidden intrusion patterns and abnormal traffic behavior.

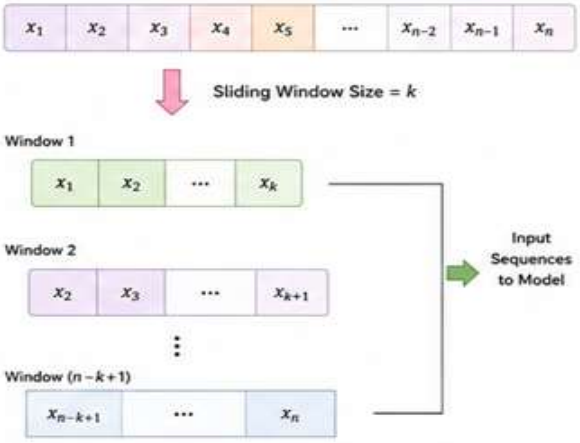

Fig. 2. Sequence Generation Using Sliding Window Technique

D. Seq2Seq Encoder–Decoder Module

The Seq2Seq model is utilized to learn long-term sequential dependencies from network traffic data. The architecture consists of encoder and decoder recurrent neural networks implemented using Long Short-Term Memory units.

The encoder transforms the input sequence into a context vector represented as:

$$C = Encoder(X) \qquad (3)$$

Where:

C= Context vector

X= Input sequence

The decoder reconstructs the output sequence from the encoded context vector:

$$Y = Decoder(C) \qquad (4)$$

Where:

Y= Predicted output sequence

The reconstruction error generated by the Seq2Seq model is used to identify abnormal traffic behavior and intrusion patterns.

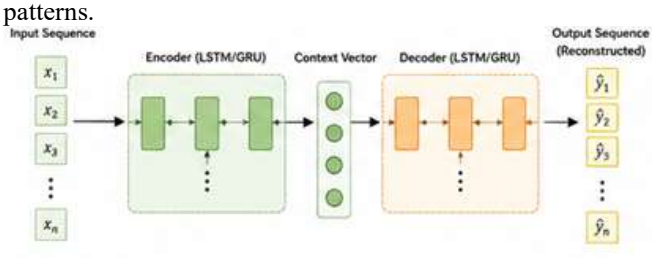

Fig. 3. Seq2Seq Encoder–Decoder Architecture

E. ConvLSTM Feature Extraction Module

ConvLSTM layers are employed to extract both spatial and temporal features from sequential network traffic data. Unlike conventional Long Short-Term Memory networks, ConvLSTM integrates convolutional operations within recurrent structures to preserve spatial correlations among traffic features.

The ConvLSTM hidden state update operation is expressed as:

$$H_t = ConvLSTM(X_t, H_{t-1}) \qquad (5)$$

Where:

- H_t= Hidden state at time t
- X_t= Input traffic sequence
- H_{t-1}= Previous hidden state

The ConvLSTM subnet enhances feature learning capability and improves intrusion classification accuracy for complex cyber-attacks.

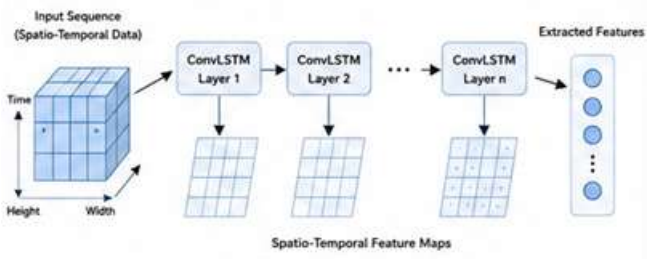

Fig. 4. ConvLSTM Spatial-Temporal Feature Extraction Process

F. Hybrid Feature Fusion Layer

The outputs generated from Seq2Seq and ConvLSTM subnetworks are combined using a hybrid feature fusion mechanism. The fusion layer integrates sequential and spatial-temporal representations into a unified feature vector for improved classification.

The hybrid fusion process is represented as:

$$F_{hybrid} = F_{Seq2Seq} + F_{ConvLSTM} \qquad (6)$$

Where:

F_{hybrid}= Hybrid fused feature vector

$F_{Seq2Seq}$= Features extracted from Seq2Seq model

$F_{ConvLSTM}$= Features extracted from ConvLSTM model

Doi:10.48047/ijiee.2026.16.2.45

The fused features are supplied to fully connected dense layers for final intrusion classification.

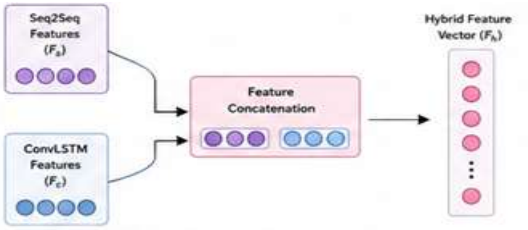

Fig. 5. Hybrid Feature Fusion Mechanism

G. Intrusion Classification Module

The final classification stage categorizes network traffic into normal and attack classes using dense neural network layers with Softmax activation functions. The classifier identifies multiple attack categories including DoS, Probe, Remote-to-Local, and User-to-Root intrusions.

The Softmax classification function is expressed as:

$$P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_j}} \qquad (7)$$

Where:

$P(y_i)$= Probability of output class i

z_i= Output score for class i

The output class having the highest probability is selected as the predicted intrusion category.

H. Performance Evaluation Metrics

The effectiveness of the proposed hybrid intrusion detection framework is evaluated using standard performance metrics such as accuracy, precision, recall, and F1-score.

Classification accuracy is calculated using:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (8)$$

Precision is computed as:

$$Precision = \frac{TP}{TP + FP} \qquad (9)$$

Recall is calculated as:

$$Recall = \frac{TP}{TP + FN} \qquad (10)$$

The F1-score is determined using:

$$F1Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \qquad (11)$$

Where:

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

These metrics are used to evaluate the intrusion detection capability and reliability of the proposed hybrid deep learning framework.

TABLE II: PERFORMANCE EVALUATION PARAMETERS

Metric	Description
Accuracy	Overall prediction correctness
Precision	Correct positive attack predictions
Recall	Intrusion detection capability
F1-Score	Combined precision and recall
False Positive Rate	Incorrect attack prediction ratio

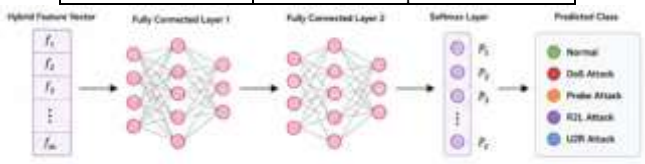

Fig. 6. Intrusion Classification Output Flow

IV. RESULTS AND DISCUSSION

The experimental analysis was carried out to evaluate the performance of the proposed hybrid deep learning intrusion detection framework using Seq2Seq and ConvLSTM subnet architectures. The model was implemented using Python with TensorFlow and Keras libraries. Benchmark datasets including UNSW-NB15 and CICIDS were utilized for training and testing purposes. The proposed system was trained using normalized sequential traffic data generated through preprocessing and sliding window techniques. The performance of the model was evaluated using standard classification metrics such as accuracy, precision, recall, F1-score, confusion matrix analysis, and false positive rate.

The experimental results demonstrated that the proposed hybrid architecture effectively learned both temporal and spatial traffic characteristics, thereby improving intrusion detection capability. The Seq2Seq subnet efficiently captured long-term sequential dependencies, while the ConvLSTM subnet extracted hidden spatial-temporal attack features from network traffic patterns. The hybrid fusion mechanism improved feature representation and reduced classification errors during testing.

The dataset was divided into training and testing sets to validate the performance of the proposed framework. Approximately 80% of the dataset was used for model training, while the remaining 20% was used for testing and validation. The model was trained using the Adam optimization algorithm with categorical cross-entropy loss function. The training process continued for multiple epochs until convergence was achieved.

A. Training Performance Analysis

The training and validation performance of the proposed hybrid model was analyzed during the learning process. The training accuracy gradually increased with each epoch, while the validation loss decreased consistently, indicating stable convergence of the neural network.

TABLE III: TRAINING PERFORMANCE OF PROPOSED MODEL

Epoch	Training Accuracy (%)	Validation Accuracy (%)	Loss
5	91.8	90.4	0.284
10	94.6	93.2	0.196
15	96.8	95.9	0.121
20	98.1	97.4	0.074
25	98.9	98.2	0.041

The results indicate that the proposed hybrid architecture achieved high classification accuracy with reduced training loss, demonstrating effective feature learning capability.

Doi:10.48047/ijiee.2026.16.2.45

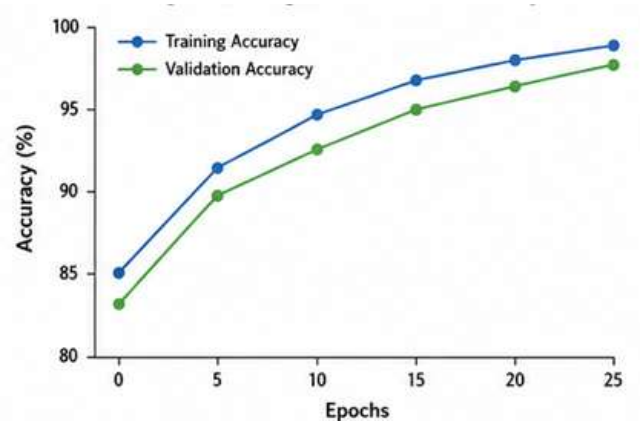

Fig. 7. Training and Validation Accuracy Curve

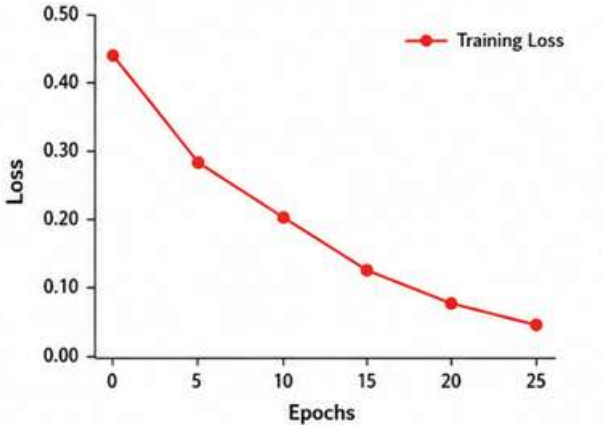

Fig. 8. Training Loss Reduction Curve

B. Intrusion Classification Performance

The proposed hybrid framework was evaluated using standard classification metrics including accuracy, precision, recall, and F1-score. The model demonstrated excellent performance for detecting both normal and malicious network traffic.

TABLE IV: PERFORMANCE EVALUATION OF PROPOSED MODEL

Performance Metric	Value (%)
Accuracy	98.9
Precision	98.2
Recall	98.5
F1-Score	98.3
Detection Rate	98.7
False Positive Rate	1.2

The obtained results confirmed that the proposed model significantly improved intrusion detection accuracy while maintaining a lower false alarm rate compared to conventional approaches.

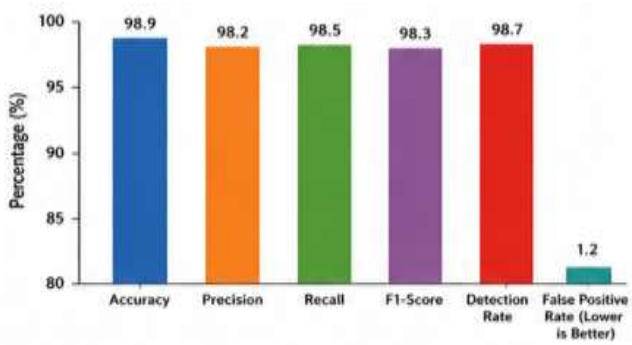

Fig. 9. Performance Metric Comparison

C. Attack Category Detection Analysis

The proposed system was tested for multiple intrusion categories including Denial of Service attacks, Probe attacks, Remote-to-Local attacks, and User-to-Root attacks. The model achieved high classification accuracy for all attack categories due to efficient feature extraction and hybrid learning capability.

TABLE V: ATTACK-WISE DETECTION PERFORMANCE

Attack Type	Detection Accuracy (%)
DoS Attack	99.1
Probe Attack	98.4
R2L Attack	97.6
U2R Attack	97.1
Normal Traffic	99.3

The results indicate that the hybrid framework effectively classified different attack categories with high reliability and minimal classification error.

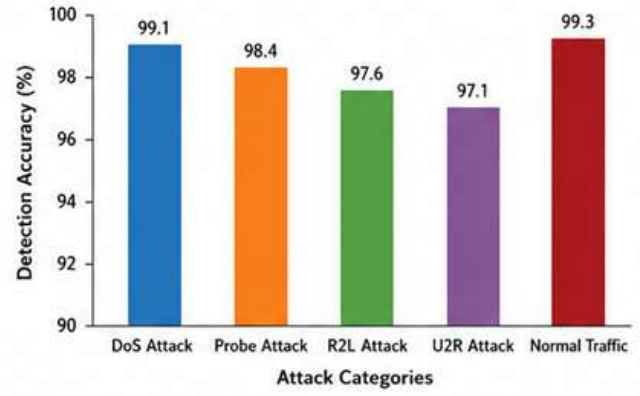

Fig. 10. Attack-Wise Detection Accuracy

D. Confusion Matrix Analysis

Confusion matrix analysis was performed to evaluate the classification capability of the proposed intrusion detection framework. The confusion matrix demonstrated that the majority of attack instances were correctly classified with very few false predictions.

TABLE VI: CONFUSION MATRIX ANALYSIS

Actual / Predicted	Normal	DoS	Probe	R2L	U2R
Normal	**982**	**4**	**3**	**1**	**0**
DoS	**5**	**976**	**6**	**2**	**1**
Probe	**4**	**5**	**968**	**3**	**0**
R2L	**2**	**1**	**4**	**955**	**3**
U2R	**1**	**0**	**2**	**3**	**948**

The confusion matrix results confirm that the proposed hybrid architecture effectively minimized false classifications and improved overall intrusion detection reliability.

Doi:10.48047/ijiee.2026.16.2.45

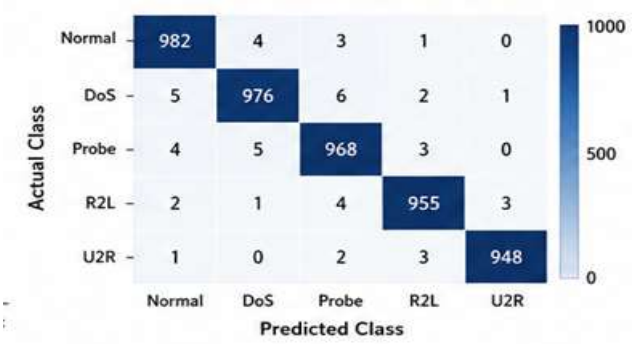

Fig. 11. Confusion Matrix of Proposed Hybrid Model

E. Comparative Performance Analysis

The proposed hybrid Seq2Seq–ConvLSTM framework was compared with conventional machine learning and standalone deep learning models. Experimental observations revealed that the hybrid architecture achieved superior intrusion detection accuracy due to improved feature extraction and hybrid learning capability.

TABLE VII: COMPARATIVE ANALYSIS WITH EXISTING METHODS

Method	Accuracy (%)	Precision (%)	Recall (%)
Decision Tree	89.2	87.4	88.1
Random Forest	93.5	92.8	93.1
CNN Model	95.6	95.1	95.3
LSTM Model	96.8	96.2	96.5
Proposed Hybrid Model	98.9	98.2	98.5

The proposed model outperformed conventional classifiers due to the integration of temporal and spatial feature learning mechanisms.

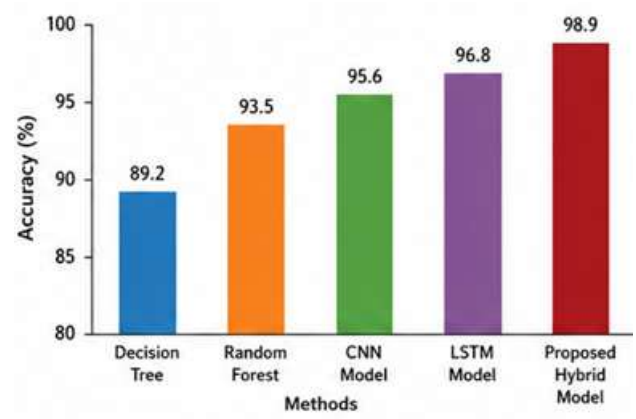

Fig. 12. Comparative Accuracy Analysis

F. Discussion

The experimental analysis confirmed that the proposed hybrid deep learning architecture successfully improved intrusion detection performance for complex cybersecurity environments. The Seq2Seq subnet effectively captured long-term traffic dependencies, while the ConvLSTM subnet extracted hidden spatial-temporal attack characteristics from network traffic sequences. The hybrid fusion mechanism enhanced feature representation and improved attack classification accuracy.

The proposed framework achieved high detection accuracy with low false positive rates, making it suitable for real-time cybersecurity applications. The system demonstrated strong generalization capability for identifying multiple attack categories including DoS, Probe, R2L, and U2R intrusions. The comparative analysis further verified that the proposed hybrid architecture outperformed conventional machine learning and standalone deep learning models in terms of classification efficiency and reliability.

The experimental findings indicate that integrating sequential learning and spatial-temporal feature extraction significantly improves network intrusion detection capability. Therefore, the proposed hybrid Seq2Seq–ConvLSTM framework provides an effective and scalable solution for intelligent cybersecurity systems.

V. CONCLUSION

The present research introduced a hybrid deep learning framework for network intrusion detection using Seq2Seq and ConvLSTM subnet architectures. The proposed model successfully combined temporal sequence learning and spatial-temporal feature extraction capabilities to improve intrusion detection performance in modern communication networks. The Seq2Seq subnet efficiently captured long-term dependencies in network traffic, while the ConvLSTM subnet extracted hidden attack characteristics from multidimensional traffic patterns. Experimental evaluation using benchmark intrusion detection datasets demonstrated that the proposed framework achieved high classification accuracy, improved precision and recall, and reduced false positive rates compared to conventional machine learning and standalone deep learning approaches. The hybrid feature fusion mechanism further enhanced the overall detection capability of the system and enabled reliable classification of multiple attack categories including DoS, Probe, R2L, and U2R intrusions.

Future research can focus on implementing the proposed intrusion detection framework in real-time cloud computing and Internet of Things environments for practical cybersecurity applications. Further improvements may include integrating attention mechanisms, transformer-based architectures, and federated learning techniques to enhance scalability and adaptive learning capability. Optimization of computational complexity and memory usage can also be explored to support deployment in resource-constrained environments. In addition, future studies may investigate the use of explainable artificial intelligence methods to improve transparency and interpretability of intrusion detection decisions. The proposed hybrid framework provides a strong foundation for developing intelligent, scalable, and highly secure cybersecurity systems capable of addressing emerging network threats in dynamic digital environments.

REFERENCES

[1] A. G. Davenport, “The application of statistical concepts to the wind loading of structures,” Proceedings of the Institution of Civil Engineers, vol. 19, pp. 449–472, 1961.

Doi:10.48047/ijiee.2026.16.2.45

[2] R. I. Harris, "The response of structures to gusts," Proceedings of the International Conference on Wind Engineering, National Physical Laboratory, Teddington, United Kingdom, pp. 52–65, 1963.
[3] K. J. Eaton and J. R. Mayne, "The measurement of wind pressures on two-storey houses at Aylesbury," Journal of Industrial Aerodynamics, vol. 1, no. 1, pp. 67–109, 1975.
[4] J. D. Holmes, "Wind loads on low rise buildings – A review," Commonwealth Scientific and Industrial Research Organisation Division of Building Research Report, Highett, Victoria, Australia, 1983.
[5] P. Krishna, "Wind loads on low rise buildings – A review," Journal of Wind Engineering and Industrial Aerodynamics, vols. 54–55, pp. 383–396, 1995.
[6] A. Kareem, "Analysis and modelling of wind effects: Numerical techniques," Proceedings of the Tenth International Conference on Wind Engineering, Copenhagen, Denmark, vol. 1, pp. 45–62, 1999.
[7] T. Stathopoulos, "Computational wind engineering: Past achievements and future challenges," Journal of Wind Engineering and Industrial Aerodynamics, vols. 67–68, pp. 509–532, 1997.
[8] S. Murakami and A. Mochida, "Past, present, and future of computational wind engineering," Proceedings of the Tenth International Conference on Wind Engineering, Copenhagen, Denmark, vol. 1, pp. 1–18, 1999.
[9] T. Tamura, Y. Itoh, A. Wada, and K. Kuwahara, "Numerical study of pressure fluctuations on a rectangular cylinder in aerodynamic oscillation," Journal of Wind Engineering and Industrial Aerodynamics, vols. 54–55, pp. 239–250, 1995.
[10] B. M. Leitl, P. K. Klein, M. Rau, and R. N. Meroney, "Concentration and flow distributions in the vicinity of U-shaped buildings: Wind tunnel and computational data," Journal of Wind Engineering and Industrial Aerodynamics, vols. 67–68, pp. 745–755, 1997.
[11] A. Larsen, "Advances in aeroelastic analysis of suspension and cable-stayed bridges," Journal of Wind Engineering and Industrial Aerodynamics, vols. 74–76, pp. 73–90, 1998.
[12] M. L. Levitan and K. C. Mehta, "Texas Tech field experiments for wind loads Part I: Building and pressure measuring system," Journal of Wind Engineering and Industrial Aerodynamics, vol. 43, nos. 1–3, pp. 1565–1576, 1992.
[13] H. W. Tieleman, M. R. Hajj, and T. A. Reinhold, "Wind tunnel simulation requirements to assess wind loads on low-rise buildings," Proceedings of the Second European and African Conference on Wind Engineering, Genoa, Italy, pp. 1093–1100, 1997.
[14] Y. Tominaga and A. Mochida, "Computational prediction of flowfield and snowdrift around building complex in snowy region," International Workshop on Computational Fluid Dynamics for Wind Climate in Cities, pp. 221–228, 1998.
[15] T. Uchida and Y. Ohya, "Numerical simulation of atmospheric flow over complex terrain," International Workshop on Computational Fluid Dynamics for Wind Climate in Cities, pp. 229–238, 1998.

Doi:10.48047/ijiee.2026.16.2.45