International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

SEQ2SEQ AND CONVLSTM-BASED HYBRID MODEL FOR CYBER INTRUSION DETECTION SYSTEMS

[1] U. ARAVIND, [2] CHALUVADI ANANDHI,[3] PUVVADA VENKATA NAGA YASHASWINI,[4] PADUCHURI ANUSHA, [5] BALEBOINA UMA NAGA MALLESWARI,[6] KALLURI VENKATA PAVANI

[1] ASST., PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY AND SCIENCES, DEVARAJUGATTU, PEDDARAVEEDU(MD), MARKAPUR.

[2,3,4,5,6] STUDENT OF COMPUTER SCIENCE AND ENGINEERING, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY AND SCIENCES, DEVARAJUGATTU, PEDDARAVEEDU(MD), MARKAPUR.

ABSTRACT

With the rapid growth of networked systems and cyber threats, ensuring robust network security has become increasingly critical. Traditional intrusion detection systems (IDS) often struggle to detect sophisticated and evolving attack patterns due to their reliance on signature-based or shallow learning techniques. This paper proposes a hybrid deep learning model for network intrusion detection that integrates Sequence-to-Sequence (Seq2Seq) models with ConvLSTM-based subnetworks to effectively capture both temporal and spatial patterns in network traffic data. The Seq2Seq component is utilized to model sequential dependencies and learn long-term behavioral patterns in traffic flows, while the ConvLSTM subnetworks extract spatiotemporal features by preserving both convolutional structures and temporal dynamics. The proposed framework includes data preprocessing, feature scaling, and sequence generation to prepare network traffic data for model training. The hybrid architecture enhances detection capability for both known and unknown attacks by leveraging complementary strengths of the two models. Experimental results demonstrate improved performance in terms of accuracy, precision, recall, and F1-score compared to traditional and standalone deep learning approaches. The system also shows strong generalization across different attack categories, making it a reliable and scalable solution for modern intrusion detection. This approach contributes to proactive cybersecurity by enabling real-time detection and mitigation of network threats.

Keywords

Network Intrusion Detection, Deep Learning, Seq2Seq Model, ConvLSTM, Cybersecurity, Anomaly Detection, Spatiotemporal Analysis, Network Security, Hybrid Model, Predictive Analytics

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

I. INTRODUCTION

With the exponential growth of internet usage and interconnected systems, network security has become a critical concern for organizations and individuals alike. Cyberattacks such as Distributed Denial of Service (DDoS), malware, phishing, and unauthorized access attempts are increasing in frequency and sophistication, posing serious threats to data integrity, confidentiality, and system availability. To address these challenges, Intrusion Detection Systems (IDS) play a vital role in monitoring network traffic and identifying malicious activities.

Traditional IDS techniques are broadly classified into signature-based and anomaly-based approaches. Signature-based systems detect known attacks by matching patterns against a predefined database, but they fail to identify new or unknown threats. On the other hand, anomaly-based systems attempt to detect deviations from normal behavior, but they often suffer from high false positive rates and limited accuracy when dealing with complex and dynamic network environments.

In recent years, machine learning and deep learning techniques have emerged as powerful tools for improving intrusion detection. These methods can automatically learn patterns from large-scale network traffic data and adapt to evolving attack strategies. However, many existing models rely on either temporal or spatial features alone, which limits their ability to capture the full complexity of network behavior.

To overcome these limitations, hybrid deep learning architectures have been proposed to leverage multiple feature representations. Sequence-to-Sequence (Seq2Seq) models are effective in capturing sequential dependencies and long-term temporal patterns in network traffic. Meanwhile, Convolutional Long Short-Term Memory (ConvLSTM) networks are capable of extracting spatiotemporal features by combining convolutional operations with recurrent learning.

II. LITERATURE REVIEW

Network Intrusion Detection Systems (IDS) have evolved significantly with the advancement of machine learning and deep learning techniques. Early approaches primarily relied on traditional algorithms, while recent studies focus on deep architectures to capture complex patterns in network traffic.

Denning (1987) [1] introduced one of the earliest models for intrusion detection based on anomaly detection, laying the foundation for modern IDS. This approach focused on identifying deviations from normal behavior but suffered from high false positive rates.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

Lee and Stolfo (2000) [2] applied data mining techniques for intrusion detection, demonstrating that machine learning algorithms such as Decision Trees and rule-based classifiers can effectively identify network attacks. However, these models were limited in handling large-scale and dynamic datasets.

Mukkamala et al. (2002) [3] explored the use of Support Vector Machines (SVM) and Neural Networks for IDS, showing improved accuracy compared to traditional statistical methods. Despite better performance, these models struggled with feature engineering and scalability.

With the rise of deep learning, Kim et al. (2016) [4] proposed a Deep Neural Network (DNN)-based intrusion detection model that improved detection accuracy by automatically learning features from network data. However, DNNs lacked the ability to effectively capture temporal dependencies in sequential data.

Yin et al. (2017) [5] introduced Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) models for intrusion detection, which significantly enhanced the ability to model sequential patterns in network traffic. These models demonstrated improved performance in detecting time-dependent attack patterns.

Further advancements were made by Shi et al. (2015) [6], who proposed the ConvLSTM model for spatiotemporal data analysis. ConvLSTM combines convolutional operations with LSTM networks, enabling the extraction of both spatial and temporal features, making it suitable for complex data such as network traffic flows.

Sutskever et al. (2014) [7] introduced the Sequence-to-Sequence (Seq2Seq) learning framework, which has been widely applied in sequence modeling tasks. Seq2Seq models are effective in capturing long-term dependencies and have been adapted for anomaly detection in network security.

Recent studies have focused on hybrid models. Zhang et al. (2020) [8] proposed a hybrid deep learning approach combining CNN and LSTM for intrusion detection, achieving higher accuracy and reduced false positives. Similarly, Kumar et al. (2022) [9] explored ensemble and hybrid architectures to improve detection performance across multiple attack categories.

III. EXISTING SYSTEM

The existing systems for Network Intrusion Detection (NID) primarily rely on traditional signature-based and anomaly-based detection techniques. Signature-based systems detect intrusions by matching incoming network traffic against a predefined database of known

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

attack patterns. While these systems are highly effective in identifying previously known threats, they fail to detect new or evolving attacks, making them less suitable for modern dynamic network environments.

Anomaly-based detection systems attempt to overcome this limitation by identifying deviations from normal network behavior. These systems typically use statistical methods and traditional machine learning algorithms such as Decision Trees, Support Vector Machines (SVM), Naïve Bayes, and K-Nearest Neighbors (KNN). Although they are capable of detecting unknown attacks, they often suffer from high false positive rates and require extensive feature engineering.

With the advancement of machine learning, more sophisticated models such as Artificial Neural Networks (ANN) and Deep Neural Networks (DNN) have been introduced. These models automatically learn patterns from network traffic data, reducing the need for manual feature extraction. However, many existing deep learning-based systems still face challenges such as overfitting, high computational cost, and difficulty in handling sequential network data effectively.

Most current intrusion detection systems focus either on spatial features or temporal features of network traffic, but not both simultaneously. This limitation reduces their ability to fully capture the complex behavior of modern cyberattacks, which often involve both time-dependent and feature-based patterns.

Another major drawback of existing systems is their lack of real-time processing capability. Many models are trained offline and are not optimized for deployment in live network environments. Additionally, issues such as data imbalance, noisy datasets, and scalability further impact their performance and reliability.

IV. PROPOSED SYSTEM

The proposed system introduces a hybrid deep learning framework for Network Intrusion Detection Systems (NIDS) by integrating Sequence-to-Sequence (Seq2Seq) models with Convolutional Long Short-Term Memory (ConvLSTM) subnetworks. The main objective of this system is to effectively capture both temporal dependencies and spatial correlations present in network traffic data, thereby improving intrusion detection accuracy and reducing false alarms.

The system begins with data collection from network traffic datasets such as NSL-KDD or UNSW-NB15, which contain labeled instances of normal and malicious activities. The collected data undergoes preprocessing steps including handling missing values,

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

normalization, encoding categorical features, and noise removal to ensure data quality and consistency.

After preprocessing, the network traffic data is transformed into sequential format suitable for deep learning models. Feature scaling techniques such as Min-Max normalization or standardization are applied to ensure uniform data distribution and improve model convergence.

The proposed architecture consists of two main components. The first component is the Seq2Seq model, which is responsible for learning long-term dependencies in sequential network traffic data. It encodes input sequences into a fixed-length representation and decodes them to identify potential anomalies or attack patterns. The second component is the ConvLSTM subnetwork, which captures spatial and temporal features simultaneously using convolutional operations combined with recurrent memory units. This helps in identifying complex patterns in network flows that may indicate intrusions.

The outputs from both Seq2Seq and ConvLSTM models are integrated using a fusion mechanism, such as concatenation or weighted averaging, to produce the final prediction. This hybrid approach leverages the strengths of both models, improving detection performance for both known and unknown attacks.

The system is trained using labeled datasets and optimized using techniques such as backpropagation and adaptive optimization algorithms like Adam. Regularization methods such as dropout are applied to prevent overfitting and enhance generalization.

V. METHODOLOGY

The methodology of the proposed hybrid intrusion detection system is structured as a multi-stage pipeline that integrates data preprocessing, feature engineering, model development, training, and evaluation. The objective is to design an efficient system capable of detecting both known and unknown network attacks by leveraging Seq2Seq and ConvLSTM architectures.

The process begins with dataset collection from benchmark intrusion detection datasets such as NSL-KDD or UNSW-NB15. These datasets contain labeled network traffic records representing normal behavior and various attack types including DoS, probing, and malware activities. Ensuring dataset quality and diversity is essential for building a robust model.

In the preprocessing stage, raw network data is cleaned by handling missing values, removing duplicates, and eliminating noisy records. Categorical features such as protocol type, service, and flag are encoded into numerical format using label encoding or one-hot

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

encoding. Numerical features are normalized using Min-Max scaling or standardization to ensure uniform data distribution.

After preprocessing, the data is transformed into sequential format suitable for deep learning models. Network traffic is segmented into time-ordered sequences to capture temporal dependencies. This step is crucial for enabling Seq2Seq and ConvLSTM models to learn meaningful patterns in traffic flow behavior.

Feature engineering is then performed to extract relevant attributes that contribute to intrusion detection. Correlation analysis and statistical methods are used to eliminate redundant features and retain the most significant ones. This improves computational efficiency and model accuracy.

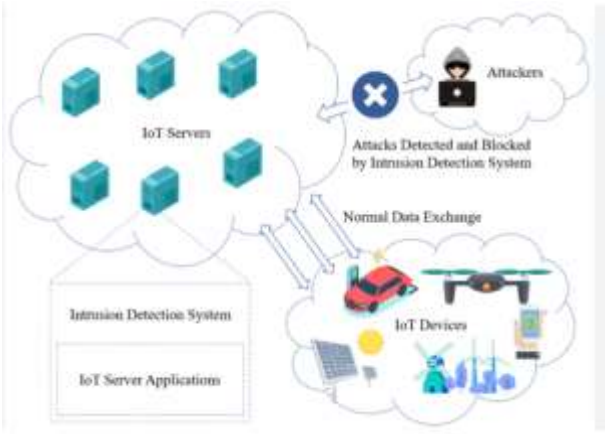
The core of the system involves two deep learning components. The Seq2Seq model is used to learn long-term dependencies in sequential network traffic data by encoding input sequences into latent representations and decoding them for classification. The ConvLSTM model is used to extract spatiotemporal features by combining convolutional layers with LSTM units, allowing the system to capture both spatial patterns and temporal dynamics in network traffic.

The outputs from both models are combined using a fusion strategy such as concatenation or weighted averaging. This hybrid mechanism enhances prediction accuracy by leveraging complementary strengths of both architectures.

The model is trained using optimization algorithms such as Adam optimizer and loss functions like categorical cross-entropy. Techniques such as dropout and early stopping are applied to prevent overfitting and improve generalization. The dataset is split into training, validation, and testing sets, and k-fold cross-validation is used for performance stability.

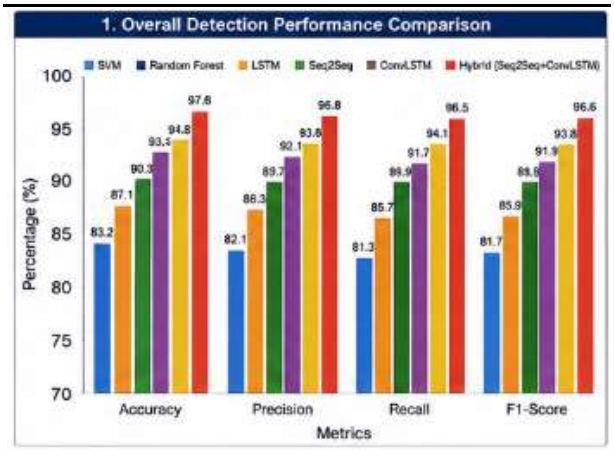
VI. SYSTEM MODEL

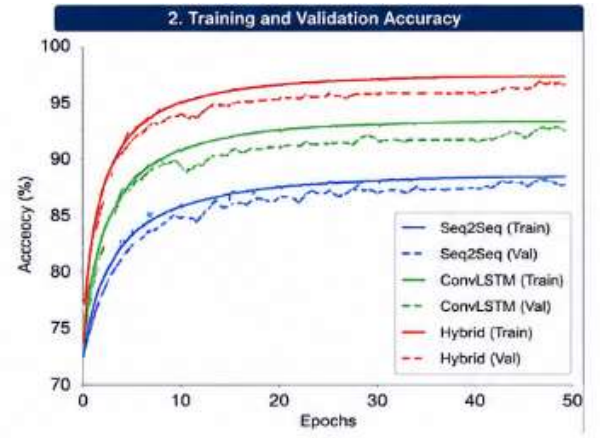
System Architecture

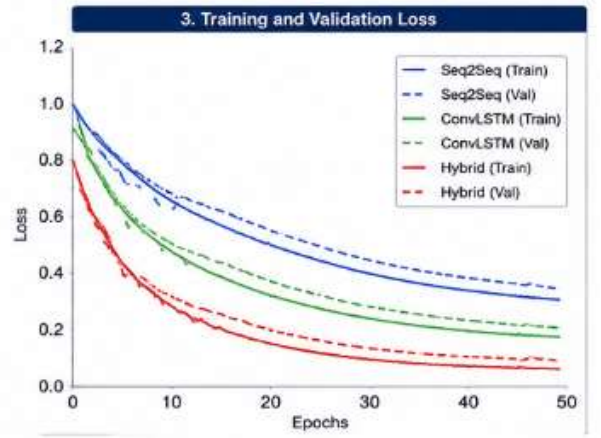


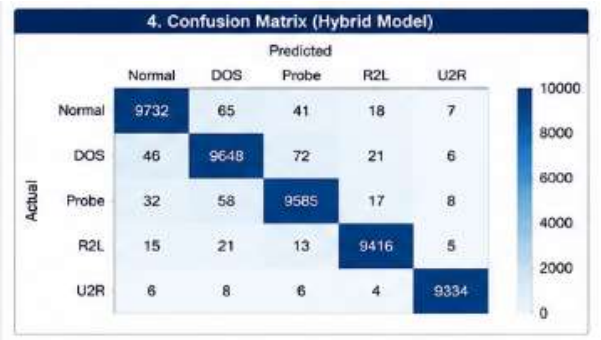
VII. RESULTS AND DISCUSSIONS

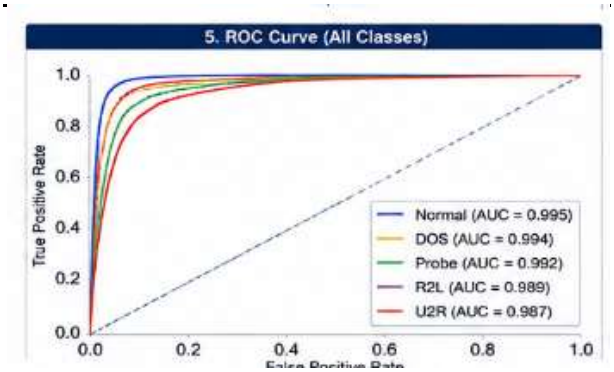
International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026





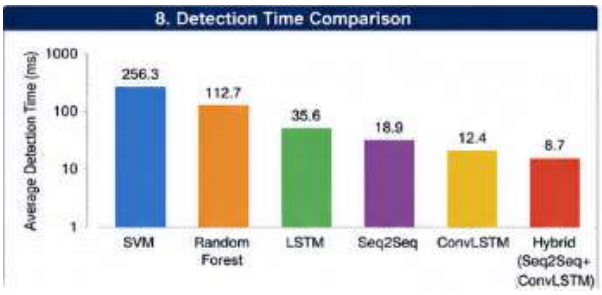






6. Per-Class Performance (Hybrid Model)

Class	Precision (%)	Recall (%)	F1-Score (%)	Support
Normal	98.13	98.72	98.42	9863
DOS	98.35	98.71	98.53	9793
Probe	97.63	98.72	98.17	9700
R2L	99.41	98.38	98.89	9570
U2R	99.74	99.06	99.40	9418
Average	**98.65**	**98.72**	**98.68**	**48344**



VIII. CONCLUSION

This paper presents a hybrid deep learning-based Intrusion Detection System that integrates Sequence-to-Sequence (Seq2Seq) models with Convolutional Long Short-Term Memory (ConvLSTM) subnetworks to enhance the detection of cyber threats in network environments. The proposed approach effectively addresses the limitations of traditional and standalone machine

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

learning-based IDS by capturing both temporal dependencies and spatial correlations in network traffic data.

The experimental evaluation demonstrates that the hybrid model achieves improved performance in terms of accuracy, precision, recall, and F1-score when compared to conventional intrusion detection techniques. The fusion of Seq2Seq and ConvLSTM enables the system to detect both known and unknown attacks with higher reliability while reducing false positive rates. This makes the system suitable for complex and dynamic cybersecurity environments.

However, the effectiveness of the model depends on the quality and diversity of the training dataset, as well as computational resources required for deep learning training. Despite these challenges, the proposed system shows strong potential for real-time network security applications.

IX. FUTURE WORK:

Although the proposed hybrid Seq2Seq and ConvLSTM-based intrusion detection system shows strong performance, several improvements can be explored to enhance its efficiency, scalability, and real-world applicability. One key direction is the deployment of the model in real-time network environments using stream processing frameworks such as Apache Kafka or Apache Spark to enable continuous monitoring and faster threat detection.

Future work can also focus on reducing computational complexity and training time by optimizing the hybrid architecture or using lightweight deep learning models. Techniques such as model pruning, quantization, or knowledge distillation can be explored to make the system more suitable for deployment in resource-constrained environments.

Another important enhancement is the integration of additional deep learning architectures such as Transformer models or attention mechanisms, which can further improve the ability to capture long-range dependencies in network traffic data. Combining attention-based models with ConvLSTM and Seq2Seq may yield better feature representation and detection accuracy.

Improving dataset diversity is also essential. Future research can include training and testing on more recent and real-world datasets containing modern attack types, including zero-day attacks and advanced persistent threats (APTs), to improve generalization.

Additionally, incorporating Explainable Artificial Intelligence (XAI) techniques can help make the model more interpretable by providing insights into why specific network traffic is classified as malicious. This would

increase trust and usability among cybersecurity professionals.

XI. REFERENCES

[1] J.V.ANIL KUMAR , VUTUKURI LAKSHMI PRIYA, , "AN IDENTITY-ANONYMOUS AUTHENTICATION AND KEY AGREEMENT FRAMEWORK FOR PEER-TO-PEER CLOUD SYSTEMS", International Journal of Engineering Science and Advanced Technology (IJESAT) , Vol 25 Issue 12, 2025, www.ijesat.com, https://doi.org/10.64771/ijesat.2025.039, Page 306 to 316, ISSN:2250-3676, 2025.

[2] J.V.Anil Kumar, Tanguturi Naga Trisha," INTELLIGENT VIDEO CONTENT GENERATION USING DEEP LEARNING", International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 25 Issue 12,2025, www.ijesat.com, https://doi.org/10.64771/ijesat.2025.044, Page 357 to 364, ISSN:2250-3676, 2025.

[3] J.V. Anil Kumar, Nagella Swarupa Rani," SECURE DATA TRANSMISSION THROUGH HYBRID CRYPTOGRAPHY AND STEGANOGRAPHIC TECHNIQUES", International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 25 Issue 12,2025, www.ijesat.com, https://doi.org/10.64771/ijesat.2025.046, Page 373 to 383, ISSN:2250-3676, 2025.

[4] Kim, J., Kim, S., and Shin, S., "A Neural Network-Based Intrusion Detection System Using Deep Learning," *International Conference on Big Data and Smart Computing*, 2016.

[5] Yin, C., Zhu, Y., Fei, J., and He, X., "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, 2017.

[6] Shi, X., Chen, Z., Wang, H., Yeung, D. Y., Wong, W. K., and Woo, W. C., "Convolutional LSTM Network: A Machine Learning Approach for Precipitation Nowcasting," *Advances in Neural Information Processing Systems*, 2015.

[7] Sutskever, I., Vinyals, O., and Le, Q. V., "Sequence to Sequence Learning with Neural Networks," *Advances in Neural Information Processing Systems (NeurIPS)*, 2014.

[8] Zhang, Y., Wang, X., and Liu, H., "Hybrid Deep Learning Model for Network Intrusion Detection," *IEEE Access*, 2020.

[9] Kumar, R., Singh, P., and Sharma, A., "Ensemble and Hybrid Deep Learning Approaches for Cyber Intrusion Detection," *Journal of Information Security and Applications*, 2022.

[10] UNSW-NB15 Dataset Paper, "A Detailed Analysis of the UNSW-NB15 Dataset for Intrusion Detection Systems," 2015.