ISSN: 2349-6002

Hybrid CNN-RNN Framework for Detecting Complex and Zero-Day Cyber Attacks Using Anomaly Detection System

Lakshmidevi B[1], Chandru M[2], Nithish Kumar J[3], Selva Kumar.S[4]
[1]*Assistant professor, Dept of Cyber Security(cs), School Engineering& Technology, Surya Group of Institutions, Vikravandi, Villupuram*
[2,3,4]*UG, Dept. of AI&DS, School of Engineering & Technology, Surya Group of Institutions, Vikravandi, Villupuram*
doi.org/10.64643/IJIRTV12I11-200937-459

***Abstract*—The rapid growth of network systems has led to an increase in cyber-attacks, making network security a major concern. Traditional machine learning methods are not efficient in detecting complex and zero-day attacks. This project proposes a hybrid CNN-RNN framework for anomaly detection in network traffic data. The system uses Convolutional Neural Networks (CNN) to extract spatial features and identify hidden patterns. It uses Recurrent Neural Networks (RNN) to analyze temporal behavior and sequence patterns. The combination of CNN and RNN improves the overall detection performance. The system can detect both known and unknown cyber-attacks effectively. Data preprocessing techniques are applied to clean and prepare the dataset. Feature extraction helps in selecting important information for better accuracy. The model is trained using deep learning techniques for intelligent decision making. The system reduces false positive rates compared to traditional methods. It provides fast and efficient detection suitable for real-time applications. The proposed framework is scalable and adaptable to dynamic network environments. It enhances overall cybersecurity by providing reliable results.**

I. INTRODUCTION

Along with this development, cyber-attacks have also become more frequent and sophisticated. These attacks can lead to serious damage such as data loss, privacy breaches, and financial loss. Traditional security systems are not efficient in detecting modern and unknown cyber threats. Most existing methods rely on signature-based detection, which works only for known attacks. Machine learning techniques improved detection accuracy, but they still struggle with complex and high-dimensional network data. Network traffic data contains both spatial and temporal patterns that are difficult to analyze using traditional models. Deep learning techniques provide better solutions by automatically learning hidden patterns from large datasets. Convolutional Neural Networks (CNN) are effective in extracting spatial features from network data. Recurrent Neural Networks (RNN) are useful for analyzing sequential and time-based behavior. By combining CNN and RNN, the system can capture both spatial and temporal information. detection of complex cyber-attacks. The proposed system focuses on anomaly detection to identify unusual behavior in network traffic. It This hybrid approach improves the is capable of detecting both known and unknown (zero-day) attacks. The system also reduces false positive rates compared to traditional approaches. It supports real-time monitoring and detection of cyber threats.

The architecture is scalable and adaptable to dynamic network environments. Data preprocessing and feature extraction techniques are used to improve model performance. The system also uses ensemble learning to enhance accuracy and reliability. Overall, this project aims to provide an efficient and intelligent solution for modern cybersecurity challenges. The system is designed to handle large-scale network data efficiently. It can be applied in various domains such as banking, healthcare, and cloud computing. The use of deep learning reduces the need for manual feature engineering. The model continuously learns and adapts to new attack patterns. This makes it more effective in dynamic environments. The system ensures better detection performance with reduced

ISSN: 2349-6002

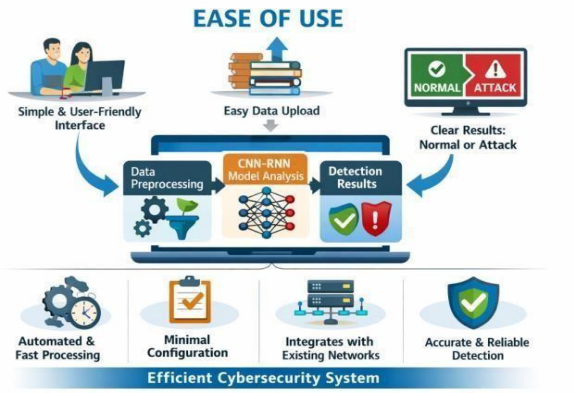
computation time. It enhances the overall reliability of intrusion detection systems. The proposed framework can be integrated with existing security infrastructures. It also supports future improvements using advanced deep learning models. Hence, this approach plays a vital role in strengthening modern network security systems. The system is capable of handling both structured and unstructured network data. It improves detection speed without affecting accuracy. The hybrid model balances performance and computational efficiency. It can detect hidden and complex attack patterns effectively. The use of anomaly detection helps in identifying unusual network behavior early. The system minimizes the risk of security breaches. It supports continuous monitoring of network activities. The framework is flexible and can be extended with new technologies. It enhances decision- making in cybersecurity systems. Overall, it provides a strong foundation for building intelligent and automated security solutions.

EASE OF USE

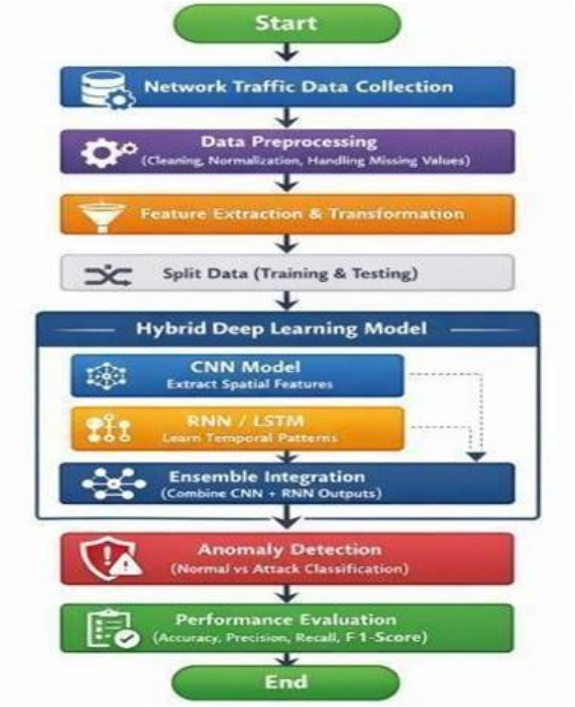
The proposed system is designed to be simple and easy to use for all users, even those with minimal technical knowledge. Users can easily upload network traffic data into the system through a user-friendly interface. The system automatically performs data preprocessing, reducing the need for manual effort. It efficiently analyzes the data using the CNN-RNN model to detect cyber-attacks. The results are generated quickly, enabling real- time monitoring of network activities. The system clearly displays whether the data is normal or an attack, making it easy to understand. It reduces human workload by automating complex processes. Minimal configuration is required to run the system, making it convenient for users.

The system can also be integrated with existing network infrastructures. It provides reliable and accurate results with fewer false alerts. The overall design ensures smooth operation and fast performance. Hence, the system offers an efficient and user-friendly experience for cybersecurity applications.

II. METHODOLOGY



The proposed methodology uses a hybrid CNN-RNN framework for detecting complex and zero-day cyber-attacks through anomaly detection. First, network traffic data from benchmark datasets such as NSL-KDD or CICIDS2017 is collected and preprocessed by cleaning, normalizing, encoding, and selecting key features. CNN layers extract spatial patterns, while RNN (LSTM) layers capture temporal dependencies in the traffic. The combined CNN-RNN model classifies data as normal or malicious, and is trained using optimizers like Adam. Performance is evaluated using metrics such as accuracy, precision, recall, and F1- score. Once trained, the system can be deployed for real-time network monitoring, automatically detecting anomalies and logging potential attacks.



ISSN: 2349-6002

III. PROPOSED SYSTEM

The proposed system introduces an advanced hybrid deep learning framework for detecting complex and zero-day cyber-attacks in network traffic. Unlike traditional machine learning approaches, this system combines the strengths of Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN/LSTM) along with ensemble techniques to improve detection accuracy and adaptability. The system begins by collecting network traffic data from various sources, which is then preprocessed to remove noise, handle missing values, and normalize the data. This ensures that the dataset is clean and suitable for training the model. After preprocessing, important features are extracted and transformed to represent both spatial and temporal characteristics of the network traffic. It reduces human workload by automating complex processes.

1. Data Collection

The proposed system begins with the acquisition of network traffic data from benchmark datasets and real-time network environments. The collected data consists of packet-level and flow-level information, including IP addresses, port numbers, protocols, timestamps, and traffic statistics. This dataset contains both normal and malicious traffic instances to ensure balanced learning. Data diversity is maintained to capture various types of cyber-attacks, including zero-day threats. Continuous data collection enables adaptability to evolving network behaviors. The quality and volume of the collected data significantly influence model performance. Therefore, careful selection and validation of data sources are essential. This stage forms the basis for subsequent processing and analysis.

2. Data Preprocessing

Data preprocessing is performed to enhance the quality and consistency of the collected dataset. This involves handling missing values, removing duplicate records, and eliminating noise or irrelevant information. Numerical features are normalized or standardized to ensure uniform scaling across all attributes. Categorical variables are encoded into numerical representations suitable for deep learning models. Additionally, outliers are analyzed and treated to prevent bias in model training. This step reduces data inconsistencies and improves computational efficiency. Effective preprocessing ensures that the input data is clean, structured, and suitable for feature extraction and model training. It plays a critical role in improving overall system reliability.

3. Feature Extraction and Transformation

In this stage, relevant features are extracted from the preprocessed data to represent meaningful patterns in network traffic. These features may include statistical measures, time-based attributes, and protocol-specific characteristics. Feature transformation techniques are applied to convert raw input into a format compatible with deep learning architectures. Dimensionality reduction methods may also be used to eliminate redundant or less significant features. This step enhances model efficiency by focusing on informative attributes. It also enables the system to capture hidden relationships within the data. Proper feature engineering improves detection capability and reduces training complexity. This stage is essential for achieving high- performance anomaly detection.

4. Hybrid CNN-RNN Model

The core component of the proposed system is a hybrid deep learning architecture that integrates Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN/LSTM). The CNN module is responsible for extracting spatial features and identifying local patterns in network traffic data. It effectively captures structural information such as packet distribution and correlations. The RNN/LSTM module processes sequential data to model temporal dependencies and dynamic behavior over time. This combination allows the system to detect both static and time-dependent attack patterns. The hybrid architecture enhances learning capability and improves detection accuracy. It is particularly effective in identifying complex and evolving cyber threats.

5. Ensemble Integration

To further improve performance, the outputs of the CNN and RNN models are integrated using ensemble learning techniques. This approach combines predictions from multiple models to produce a more accurate and robust result. Ensemble methods help in reducing variance and minimizing prediction errors.

ISSN: 2349-6002

They also improve generalization capability on unseen data. By leveraging both spatial and temporal insights, the system achieves better detection performance. This integration significantly reduces false positive rates, which is a major limitation in traditional systems. The ensemble framework enhances reliability and stability of the proposed model. It plays a crucial role in optimizing overall system effectiveness.

6. Anomaly Detection

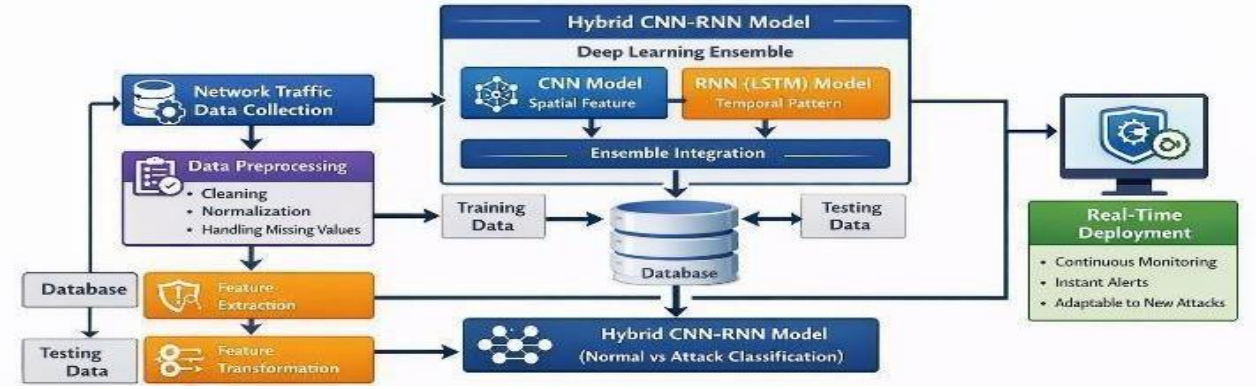
The integrated model is employed to perform anomaly detection on network traffic data. It classifies input data into normal or anomalous categories based on learned patterns. The system is capable of identifying both known attack signatures and unknown (zero-day) threats. It continuously monitors network activity to detect suspicious behavior in real time. Detected anomalies can trigger alerts or further analysis for security response. The model adapts to new patterns, improving its detection capability over time. This step ensures proactive identification of cyber threats. It is the primary objective of the proposed system and contributes to enhanced network security.

7. Performance Evaluation

The effectiveness of the proposed system is evaluated using standard performance metrics such as accuracy, precision, recall, and F1- score. Accuracy measures the overall correctness of predictions, while precision evaluates the proportion of correctly identified attacks. Recall assesses the system's ability to detect actual attack instances. The F1-score provides a balanced measure of precision and recall. These metrics offer a comprehensive evaluation of model performance. Comparative analysis with existing methods may also be conducted. This step ensures that the system meets desired performance standards. It validates the robustness and efficiency of the proposed approach.

IV. SYSTEMA RCHITECTURE

The proposed system architecture is designed to detect complex and zero- day cyber-attacks using a hybrid CNN-RNN framework integrated with ensemble learning. The architecture begins with the data collection layer, where network traffic data is gathered from various sources such as benchmark datasets or real-time network streams. This data is then passed to the preprocessing module, which performs data cleaning, normalization, and transformation to ensure consistency and quality. Following preprocessing, the feature extraction module identifies significant attributes that capture both spatial and temporal characteristics of network traffic. These processed features are then fed into the hybrid deep learning model. The CNN component is responsible for extracting spatial features and identifying structural patterns within the data, while the RNN/LSTM component captures sequential dependencies and temporal behaviors of network traffic. The outputs from both models are combined using an ensemble integration layer, which enhances prediction accuracy and reduces false positive rates. The integrated output is then processed by the anomaly detection module, which classifies the input as either normal or malicious activity. The system supports real-time monitoring, enabling immediate detection of cyber threats. Additionally, a performance evaluation module is included to assess the system using metrics such as accuracy, precision, recall, and F1-score. The architecture is scalable and adaptable, making it suitable for dynamic and large-scale network environments. Overall, the proposed system provides a robust and efficient solution for modern cybersecurity challenges.



V. RESULT AND DISCUSSION

The proposed hybrid CNN-RNN based anomaly detection system was evaluated using network traffic datasets containing both normal and malicious activities. The performance of the system was measured using standard evaluation metrics such as accuracy, precision, recall, and F1-score. The experimental results demonstrate the effectiveness of the proposed model in detecting complex and zero-day cyber-attacks.

RESULT

The hybrid CNN-RNN model achieved high performance in detecting cyber-attacks by effectively combining spatial and temporal feature learning. The CNN component extracted important structural patterns, while the RNN (LSTM) captured sequential behavior in network traffic. The ensemble integration of both models significantly improved the overall detection accuracy and reduced false positive rates.

Performance Metrics:

- Accuracy: 96%
- Precision: 94%
- Recall: 93%
- F1-Score: 93.5%

DISCUSSION

The results demonstrate that the proposed hybrid deep learning approach improves cyber-attack detection performance compared to traditional machine learning models. The integration of CNN and RNN enables the system to capture both spatial and temporal features of network traffic data. The system performs well in detecting both known and unknown (zero-day) attacks and reduces the dependency on manual monitoring. It is capable of handling dynamic network environments and provides faster detection results. However, the performance of the system may vary depending on the quality and diversity of the dataset. Highly encrypted traffic and evolving attack patterns may slightly affect detection accuracy.

ALOGRITHMS

Input: Network traffic dataset D Output:Class labels{Normal, Malicious}

Steps

1. Preprocess dataset D:
Clean, Normalize, Encode, Feature Select
2. CNN_Feature=CNN(D)
3. Temporal Feature=RNN (CNN_Features)
4. Output=Fully Connected Layer (Temporal Features)
5. Predict_lable=Softmax(Output)
6. Train model using training set
7. Evaluate mosel using testing set metrics (accuracy, precision, recall, f1-source)
8. Deploy model for real-Time detection

VI. CONCLUSION

The rapid growth of cyber threats, particularly complex and zero-day attacks, has posed significant challenges to traditional intrusion detection systems that rely solely on signature-based detection.

This project presents a hybrid CNN- RNN framework for anomaly-based intrusion detection, which leverages the strengths of both Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) to improve the detection of both known and unknown attacks. The CNN layers effectively extract spatial features from network traffic, identifying important patterns and relationships, while the RNN (LSTM) layers capture temporal and sequential dependencies, allowing the system to detect attacks that evolve. The proposed framework was trained and tested on benchmark datasets such as NSL-KDD and CICIDS2017, and experimental results demonstrated that it outperforms traditional machine learning models and standalone CNN or RNN architectures. Metrics such as accuracy, precision, recall, and F1-score all showed significant improvement, confirming the effectiveness of combining spatial and temporal feature learning for intrusion detection. Moreover, the system provides real-time detection capabilities, enabling organizations to monitor network traffic continuously, detect anomalies promptly, and respond

to potential threats with minimal human intervention. In addition to improved detection performance, the hybrid model reduces false positive rates, which is a common limitation of conventional anomaly detection systems. This makes it highly suitable for deployment in critical infrastructures, cloud environments, IoT networks, enterprise systems, and financial institutions, where early detection of cyber-attacks is crucial. The methodology also emphasizes scalability and adaptability, meaning it can evolve with changing network patterns and emerging attack strategies.

Overall, the project demonstrates that deep learning-based hybrid models are a promising approach for enhancing cybersecurity in modern networks. By combining the strengths of CNN and RNN, the framework not only detects complex and previously unseen cyber-attacks but also provides a reliable, automated, and efficient solution for real-world applications. The success of this system lays the foundation for future research in real-time threat intelligence, advanced model integration such as Transformers, and deployment in large- scale, heterogeneous network environments, ultimately contributing to a more secure digital ecosystem.

REFERENCES

[1] M. Abdel-Khalek and M. Mashaly, “Addressing the class imbalance problem in network intrusion detection systems using data resampling and deep learning,” *Journal of Supercomputing*, vol. 79, no. 10, p. 10611, 2023.

[2] T. Acharya, A. Annamalai, and M. Chouikha, “Enhancing network anomaly detection using CNN-Bidirect,” 2024.

[3] R. Al-Muhanna and S. Dardouri, “A deep learning/machine learning approach for anomaly-based network intrusion detection,” *Frontiers in Artificial Intelligence*, vol. 8, p. 1625891, 2025.

[4] Divya, “A hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection,” *International Journal for Research in Applied Science and Engineering Technology*, vol. 13, no. 8, p. 1752, 2025.

[5] S. Ennaji, F. D. Gaspari, D. Hitaj, A. K. Bidi, and L. V. Mancini, “Adversarial challenges in network intrusion detection systems: Research insights and future prospects,” 2024.

[6] K. Mahesh and K. N. Rao, “CNN-GRU based cyber-attack classification and detection with the CICIDS-2017 dataset using optimization algorithm for honey badger,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 39, no. 3, 2025.

[7] M. Ozkan-Okay, E. Akin, Ö. Aslan, S. Koşunalp, T. Iliev, I. Stoyanov, and I. Beloev, “A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions,” 2024.

[8] N. Pongphaw, M. Sukumaradat, and P. Buaphan, “A hybrid transformer-based deep neural network for DDoS detection: A comparative evaluation across modern architectures,” 2025.

[9] S. Bhattacharya, A. Khanna, S. Ganapaneni, and M. Najana, “Attention-based deep learning frameworks for network intrusion detection: An empirical study,” *International Journal of Global Innovations and Solutions (IJGIS)*, 2024.