**NETWORK INTRUSION DETECTION SYSTEM USING HYBRID DEEP LEARNING**

**R. Karthick1, L. Arun Prasath2, J. Mohammad Zayed Rahman3, S. Abisheik4, A. Nambi Raja5,**

*1Associate Professor Department of Computer Science and Engineering, K.L.N. College of Engineering, Sivagangai, Tamilnadu, India.*

*2,3,4,5 Final Year Students, Department of Computer Science and Engineering, K.L.N. College of Engineering, Sivagangai, Tamilnadu, India.*

**Abstract:** This Network Intrusion Detection System (NIDS) are essential for safeguarding computer networks, analyzing traffic to detect malicious activities. With increasing network traffic and sophisticated cyber-attacks, traditional rule- and signature-based IDS struggle with scalability and adaptability. This research examines the use of hybrid deep learning techniques—like Convolutional Neural Networks (CNNs) combined with Bidirectional Long Short-Term Memory (BiLSTM)—to enhance NIDS capabilities in detecting both known and unknown attacks. Recent advancements demonstrate that deep learning-based NIDS improve detection accuracy and reduce false positives, offering a robust and scalable solution for network security.

**Keywords:** Convolutional Neural Network, Anomaly detection, Cyber-attacks, Deep learning, Network Security

# **I. INTRODUCTION**

Intrusion Detection monitors network and system activity to detect malicious or abnormal behavior. Intrusion Detection Systems (IDS) are either host-based (HIDS), monitoring individual computers, or network-based (NIDS), analyzing network traffic. NIDS use two main detection methods: signature-based, which matches known attack patterns but can’t detect new (zero-day) threats, and anomaly-based, which identifies unusual behavior for improved zero-day detection but may trigger false alarms. Adding NIDS enhances cybersecurity by providing an extra layer of defense against potential threats.

## **II. OBJECTIVE**

By using hybrid deep learning models, this research aims to improve Network Intrusion Detection Systems (NIDS) and increase their scalability, adaptability, and accuracy in identifying cyberthreats. In particular, it seeks to detect both known and unknown (zero-day) attacks by utilizing Convolutional Neural Networks (CNNs) and Bidirectional Long Short-Term Memory (BiLSTM) models to identify intricate patterns in network traffic. Enhancing real-time efficiency and scalability to manage large data volumes with low latency is the main goal of this strategy. By strengthening the model's capacity to discriminate between malicious and benign activity, the system's precision will be increased and false positive rates will be decreased. Furthermore, the study aims to develop a generalizable and flexible NIDS that can operate in a variety of network environments.

## **III. LITERAURE SURVEY**

1. **Current method for Network Intrusion Detection System:**

In order to increase detection accuracy and decrease false positives, this paper proposes a novel method for improving Network Intrusion Detection Systems (NIDS) using Generative Adversarial Networks (GANs). The hybrid model overcomes the drawbacks of conventional signature-based systems by producing synthetic data that imitates malicious and legitimate traffic, improving the ability to identify new threats. The approach, which uses a generator and discriminator for adversarial training, has been shown to increase detection rates, decrease false positives, and be scalable across different network environments. To improve the model's real-time detection capabilities, more research is advised.

1. **Detection Systems with Deep Learning:**

The use of deep learning techniques to improve Intrusion Detection Systems (IDS) for increased network security is examined in this paper. It examines several architectures, including Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNNs), emphasizing their better detection rates and real-time processing capabilities in comparison to conventional techniques. Even though deep learning models can continuously learn to adapt to changing threats, problems with interpretability and high computational requirements still exist. To increase efficacy and transparency, the authors propose future research avenues that include explainable AI (XAI) integration and hybrid models.

## **IV. EXISTING SYSTEM**

Programming education is undergoing a revolution thanks to automated assessment systems and data mining techniques, which provide predictive analytics, individualized learning experiences, and thorough insights into student performance. But conventional approaches frequently lack hands-on coding experience, necessitating a more efficient strategy. We suggest OptiCode, a cutting-edge approach created to close this gap by improving accessibility and efficacy in programming skill acquisition.

**V. PROPOSED SYSTEM**

By incorporating cutting-edge AI techniques for individualized learning and code improvement, OptiCode is a creative system that improves programming education. After users choose a programming language and subject, Jina Embedding converts their queries into numerical vectors. Large Language Models (LLMs) and Retrieval Augmented Generation (RAG) are used by the system to produce precise code snippets that enable interactive optimizations and corrections. By utilizing real-time data, this all-inclusive workflow creates an immersive learning environment and raises the bar for programming education.

## **VI. ARCHITECTURE DIAGRAM**

***Fig 6.1 Architecture Diagram***

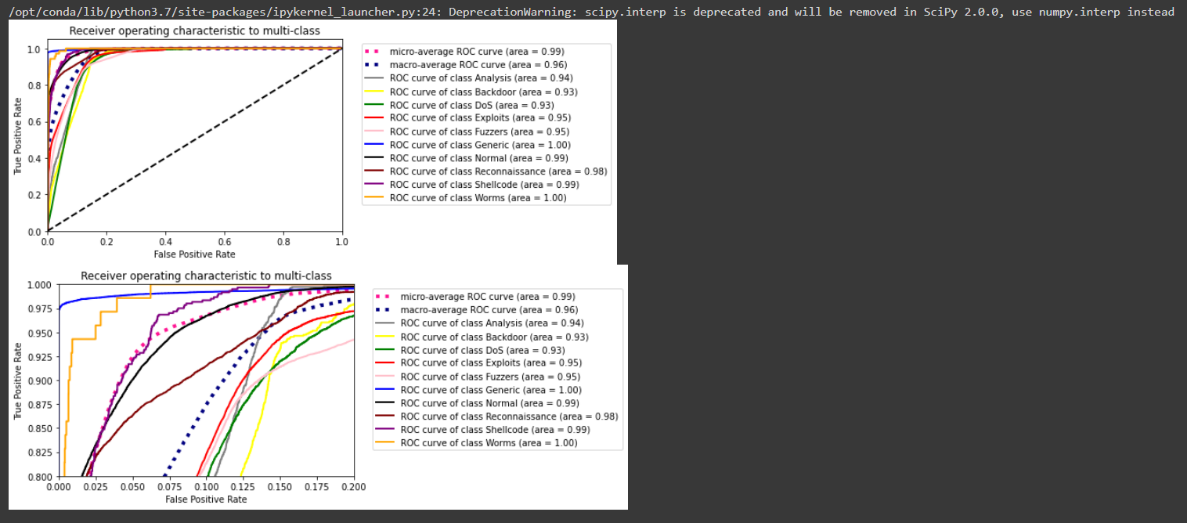
## **VII. SYSTEM OVERVIEW**

### **1. Data Preprocessing**

Data Preprocessing is done because it converts unstructured network traffic data into a clean, organized format, data preprocessing is essential to developing a successful Network Intrusion Detection System (NIDS) with hybrid deep learning. To improve the model's anomaly detection capabilities, this entails data cleaning, feature encoding, normalization, and resolving imbalanced datasets. A solid foundation for the intrusion detection pipeline is provided by appropriate preprocessing, which increases training efficiency and decreases overfitting.

**2. Dimensionality Reduction**

By narrowing the feature space in big datasets, dimensionality reduction is essential for creating effective and scalable Network Intrusion Detection Systems (NIDS). Autoencoders efficiently compress data, t-distributed Stochastic Neighbor Embedding (t-SNE) helps visualize data relationships, and Principal Component Analysis (PCA) maximizes variance while increasing efficiency. All things considered, these techniques improve interpretability and model performance, enabling the NIDS to handle large amounts of network traffic while preserving high detection accuracy.



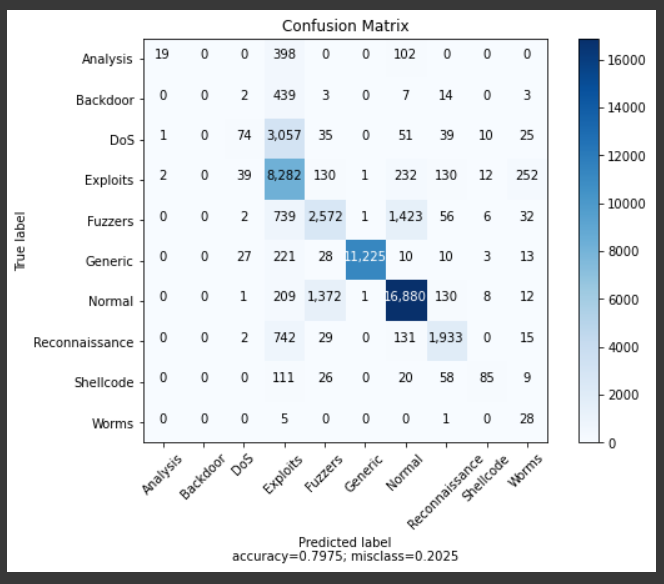
***Fig 7.1 Data Preprocessing and Dimensionality Reduction Result***

1. **BILSTM Sequential Analysis**

Data Preprocessing is done because it converts unstructured network traffic data into a clean, organized format, data preprocessing is essential to developing a successful Network Intrusion Detection System (NIDS) with hybrid deep learning. To improve the model's anomaly detection capabilities, this entails data cleaning, feature encoding, normalization, and resolving imbalanced datasets. A solid foundation for the intrusion detection pipeline is provided by appropriate preprocessing, which increases training efficiency and decreases overfitting.

1. **Intrusion Detection and Alerting**

The NIDS's Intrusion Detection and Alerting module examines network traffic for anomalies suggestive of possible threats using a hybrid CNN and BiLSTM model. It creates alerts in real time to alert administrators through channels that can be customized, allowing for quick actions to minimize damage. The module balances false positives and detection rates using a threshold-based scoring system. This all-encompassing strategy improves threat analysis and fortifies network security management in general.



***Fig 7.2 Pictorial Representation of Detection and Alerting***

**IX. FUTURE ENHANCEMENT**

A number of enhancements can be made to the Network Intrusion Detection System (NIDS) using hybrid deep learning to improve its functionality and performance. The model's generalizability across a range of network environments can be improved by incorporating additional datasets, such as KDD99, and contemporary traffic sources, which will help detect different kinds of traffic. The detection of unknown or novel attacks may be enhanced by combining unsupervised learning techniques with the current supervised CNN-BiLSTM architecture. Additionally, optimizing input features through the use of feature selection techniques like Recursive Feature Elimination (RFE) would increase accuracy while lowering computational complexity. Lastly, implementing the system in a distributed setting, like cloud or edge computing, would improve scalability and responsiveness by allowing real-time processing of massive network traffic.

**X. CONCLUSION**

A reliable and effective solution for real-time intrusion detection is offered by the Network Intrusion Detection System (NIDS), which uses hybrid deep learning to combine Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (BiLSTM). This model accurately identifies known and unknown threats, such as Denial of Service (DoS), Distributed Denial of Service (DDoS), and port scanning attacks, by utilizing the temporal pattern recognition strengths of BiLSTMs and the spatial feature extraction capabilities of CNNs. To sum up, this hybrid NIDS offers a scalable, flexible, and trustworthy method of handling contemporary network security issues.

# **REFERENCES**

*[1] Al-QatfM. I. A., M. Lasheng, M. O. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," IEEE Access, vol. 6, pp. 52843-52856, Sep. 2018.*

*[2] AltwaijryN, TuraikiAl , "A convolutional neural network for improved anomaly-based network intrusion detection," Big Data, vol. 9, no. 3, pp. 233-252, Jun. 2021*

*[3] Alam.M, Javaid. A, Niyaz. Q &Sun. W, "A deep learning approach for network intrusion detection system," Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), pp. 21-26, Dec. 2015.*

*[4] Bailey. D.H,Zhang. Y, Xie. N, Wang. W &Li. X , "Deep learning based network intrusion detection system with feature selection method," IEEE Access, vol. 7, pp. 18560-18575, Feb. 2019.*

*[5] Chehri. A,Quy. V.K, Quy. N.M, Han. N.D, and Ban. N.T, "Innovative trends in the 6G Era: A comprehensive survey of architecture, applications, technologies, and challenges," IEEE Access, vol. 11, pp. 39824-39844, 2023.*

*[6] Lashkari. A.HSharafaldin. M, and Ghorbani. A.A, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), pp. 108-116, Jan. 2018.*

*[7] Lasheng. M, Al-Qatf. M.I.A, Al-Habib. M.O, and Al-Sabahi. K, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," IEEE Access, vol. 6, pp. 52843-52856, Sep. 2018.*

*[8] Pandey. M et al., "The transformational role of GPU computing and deep learning in drug discovery." Nat. Mach. Intell., vol. 4, no. 3. pp. 211-221, 2022.*

*[9] Yin. Z, and Zhu. Z, "A hybrid model using deep auto-encoder and one-class SVM for anomaly detection," Knowledge-Based Systems, vol. 195, no. 1, 105648, Apr. 2020.*