IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511188

NeuroSecure: Deep Learning for Cyber Defense

Narasimharaju Paka[1], P Anirudh[2], B Adarsh Reddy[3], G Raghavendra[4], K Naveen Kumar[5]

Assistant Professor, Department of CSE, BITM Ballari[1]

Department of CSE, BITM Ballari[2-5]

Abstract: Historically, NeuroSecure: Deep Learning for CyberDefense have played a vital role in safeguarding network infrastructures against cyberattacks. Early NeuroSecure solutions predominantly relied on signature-based detection techniques, which were effective for identifying known attack patterns but exhibited significant limitations when confronted with zero-day attacks, polymorphic malware, and adaptive or moving-target threats. To mitigate these shortcomings, anomaly-based detection methods were introduced to identify deviations from normal network behavior. Although anomaly-based NeuroSecure improved the detection of previously unseen attacks, they often suffered from high false-positive rates and limited contextual awareness. With the increasing complexity and scale of modern cyber threats, deep learning (DL) techniques have emerged as a powerful paradigm for NeuroSecure. Deep learning-based are capable of automatically learning hierarchical and high-level representations from high-dimensional network traffic data, leveraging advances in computational resources and neural network architectures. In this paper, we propose a robust hybrid DL-NeuroSecure framework that integrates both signature-based and anomaly-based detection mechanisms, further strengthened through an ensemble of deep learning models. Unlike traditional approaches that rely on classical machine learning algorithms, the proposed system exclusively employs deep neural networks. Specifically, convolutional neural networks (CNNs) are utilized to capture spatial feature representations, recurrent neural networks (RNNs) to model temporal dependencies in sequential traffic data, and Transformer models to extract context-aware features using attention mechanisms. Each model is independently trained on benchmark datasets, including NSL-KDD and CICIDS2017, following comprehensive data preprocessing, normalization, and feature encoding procedures. To enhance detection robustness and reduce model bias, a majority-voting fusion layer is employed to aggregate predictions from the individual deep learning models. This ensemble strategy improves stability and resilience across diverse and evolving attack scenarios. Experimental evaluations demonstrate that the proposed ensemble DL-NeuroSecure achieves detection accuracy exceeding 96%, with precision, recall, and F1-score consistently surpassing 94% across all attack categories. The attention-based Transformer component significantly enhances generalization to previously unseen threats, while the CNN and RNN branches effectively capture complementary spatial and temporal characteristics of network traffic. Furthermore, the modular and scalable architecture of the proposed system makes it well suited for enterprise-scale networks, cloud-based environments, and real-time intrusion monitoring, offering low-latency processing and the ability to handle high-volume traffic streams. In addition, the proposed framework effectively addresses key challenges in detection, including class imbalance, feature redundancy, and the high dimensionality of network traffic data. Overall, this work demonstrates the practical viability and effectiveness of modern deep learning techniques in detection. By combining hybrid detection strategies with ensemble deep learning architectures, the proposed system achieves high accuracy, robustness, and operational reliability for real-world cybersecurity applications.

Keywords: NeuroSecure: Deep Learning for Cyber Defense, Deep Learning, CNN, RNN, Transformer Model, Network Security, NSL-KDD, CICIDS2017, Ensemble Architecture, Cybersecurity

I. INTRODUCTION

In our digitally interconnected world, the volume and complexity of cyber threats are growing at an increasing pace. The rise of online services, public clouds, smart devices and remote working has already laid bare network infrastructures to ongoing vulnerabilities. Traditional security tools like firewall, antiviruses and static filters are ineffective against advanced attacks that can evade or manipulate pre-defined rules. Hence, adaptive, intelligent and autodidactic security mechanisms are of increased importance. In next-generation defines systems, **NeuroSecure: Deep Learning for CyberDefense** are the most highlighted technology for detecting unauthorised access and anomalies in network behaviours.

NeuroSecure have been traditionally classified into two categories: signature-based and anomaly-based. Signature-based IDS work by comparing the network traffic with predefined attack patterns in a signature database and they look for the attack patterns in the traffic packet. While such models work well for known attacks, they do not detect novel or changing threats like zero-day breaches. In contrast, anomaly-based **NeuroSecure** create a profile of normal activities

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511188

and then detect anomalies as potential attacks. Although effective at detecting unknown threats, anomaly-based systems are plagued with high false positive rates and their accuracy varies greatly over time. Both approaches suffer from limitations when used separately in dynamic, large-scale environments that attack patterns keep evolving.

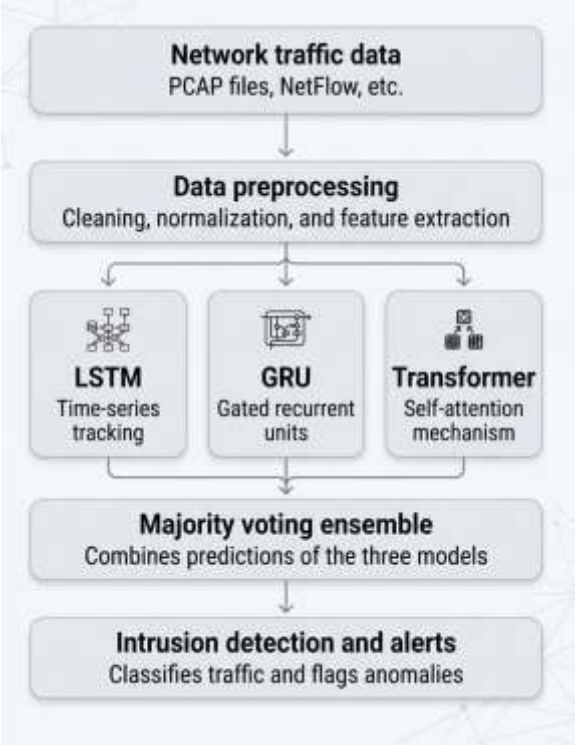
Recent advances have moved the focus of research towards the incorporation of Deep Learning (DL) frameworks in order to address these limitations. Deep learning techniques, including CNNs, RNNs and Transformer architectures have been proven to be effective in learning intricate spatial-temporal-contextual representations from raw network traffic (Wang et al. 2019). These methods automatically learn deep feature representations, thus allowing the system to distinguish more accurately between intruder activity and normal behaviour. Deep ensemble approaches, by assembling a number of DL models, have also demonstrated higher robustness and fewer false alarms as well as a superior generalisation towards never-before-seen threats.

NeuroSecur based on deep learning techniques extensively leverage preprocessing layers [24] comprising feature scaling, traffic encoding and even data dimensionality reduction in some cases to be able to operate profitably over large network data. The NSL-KDD and CICIDS2017 benchmark datasets commonly employed in training DL-based IDS configurations are representative of real-world traffic and encompass a range of attack types

The work presents a hybrid deep-learning based detection system, integrating the merits of both anomaly-based and signature-based detection methods through the use of deep ensemble classification method. In contrast to the traditional machine-learning classifiers (@20949), we adopt CNN, RNN, and Transformer models in our proposed system, which are further combined by a majority voting rule for attack detection with a higher accuracy and fewer false positives. The performance of the system is tested using NSL-KDD and CICIDS2017 datasets based on accuracy, precision, recall, and F1-score. The aim is to provide a scalable, precise and real-time solution for IDS that can be used in an enterprise, cloud and high-throughput setting.

Remaining of the paper is organized as follows: literature review, experimental methodology, results and future improvements for the system.

II. SYSTEM STRUCTURE



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511188

III. METHODOLOGY

The primary objective of this study is to design and develop a robust hybrid **NeuroSecure: Deep Learning for CyberDefense** that leverages the combined strengths of multiple machine learning and deep learning classifiers to enhance overall network security. The proposed aims to overcome the limitations of traditional signature-based and single-model detection systems, particularly in identifying sophisticated, evolving, and previously unseen cyberattacks while minimizing false-positive rates.

To ensure comprehensive evaluation and real-world applicability, the system is trained and validated using two widely recognized benchmark datasets: NSL-KDD and CICIDS2017. These datasets are extensively used in intrusion detection research due to their rich feature sets, well-labeled attack categories, and inclusion of realistic network traffic patterns that reflect modern cyber threats. NSL-KDD provides a refined version of earlier datasets by eliminating redundancy and bias, while CICIDS2017 offers contemporary traffic behavior with a wide range of attack scenarios.

By utilizing these datasets, the study aims to rigorously assess the effectiveness, generalization capability, and reliability of the proposed across diverse attack types and network conditions. Ultimately, the goal is to develop an intelligent, scalable, and deployable detection framework capable of improving threat detection accuracy and strengthening security in dynamic network environments.

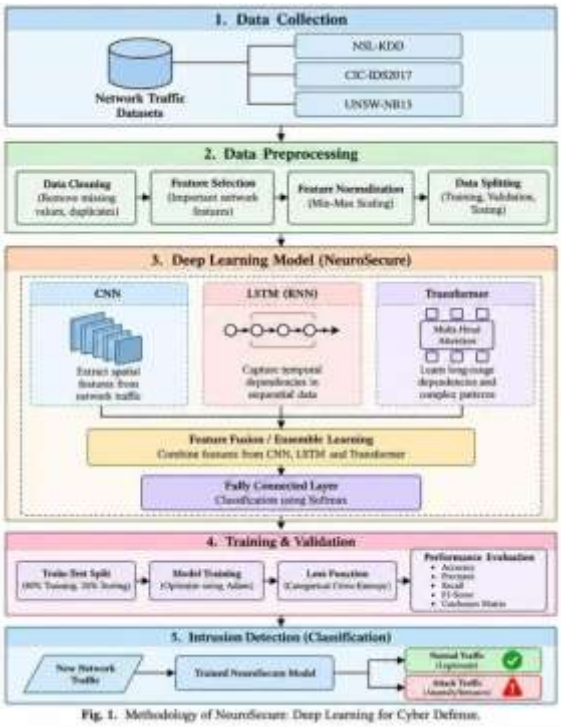


Fig. 1. Methodology of NeuroSecure: Deep Learning for Cyber Defense.

A. Dataset Collection and Preprocessing

The NSL-KDD dataset, an enhanced version of the KDD'99 dataset, contains labelled traffic segments categorized as normal or various attack types (e.g., DoS, R2L, U2R, Probe). It offers contemporary traffic patterns and modern attack scenarios like botnets and brute-force attacks, making it suitable for training robust models.

Before feeding the data into machine learning models, several preprocessing steps were carried out:

Data Cleaning: Eliminated missing values and redundant records.

Label Encoding: Converted categorical labels (e.g., attack types) into numeric representations.

Feature Selection: Removed irrelevant or low-impact features using correlation matrices and chi-square tests.

Normalization: Scaled feature values to ensure uniformity across dimensions.

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026
DOI: 10.17148/IJARCCE.2026.1511188

B. Knowledge Refinement and Feature Engineering To enhance model learning, additional features such as connection rate, protocol entropy, and flag combinations were engineered. Feature importance was evaluated using ensemble-based estimators like Random Forests, retaining only the most relevant features. Dimensionality reduction techniques like PCA were explored to mitigate overfitting and reduce computational complexity.

C. Model Construction and Ensemble Framework The system model uses a deep-learning based ensemble framework involving three Android-Net model, which captures different behavioural patterns of traffic. The first block is formed by a CNN that is good at learning spatial-local feature patterns based on structured network flow representations. CNNs are well-suited when it comes to detecting the hidden presence of invariance requests, automatically combining multi-level attack signatures from traffic matrices based or packet's captured sequences. The second part makes use of a Recurrent Neural Network (RNN) to capture temporal patterns in the active state sequence. Since a lot of the intrusions leave some characteristic temporal patterns, RNN is good at identifying anomalous sequences which makes them very useful for time based traffic logs. Third part contains a Transformer-based model using self-attention mechanism to capture both the long-distance dependencies, and context-based relationships over all network traffic sequence. This enables the model to learn higher-level attack actions, which may not be well represented by local or short-term features

All the trained deep learning models are then used to produce multiple outputs that provide several different views of representing features within the ensemble. At the prediction time, all model's outputs are combined by majority-voting approach to aggregate: the election of final class decision is based on the most-predicted label among all ensemble members. Such a method greatly enhances the robustness of reliability by mitigating mis-classification from any single model and the performance of overall **NeuroSecure** detection. The proposed approach derives the benefit of CNN, RNN, and Transformer models leading to better accuracy, generalization as well as robust against known and unknown cyber threats.

D. System Deployment and Real-Time Classification The trained ensemble model is integrated into a real-time detection framework. A user-friendly web interface enables users or administrators to upload network logs or monitor live traffic. Python (with scikit-learn and Flask) powers the backend for input classification and threat label assignment with associated confidence scores. The modular design ensures seamless updates and integration into existing security setups.

IV. RESULTS

To evaluate the effectiveness of the proposed hybrid **NeuroSecure** framework, various performance metrics were utilized to gain unique insights into the model's detection capabilities and operational reliability. The assessment was carried out on two standard datasets, NSL-KDD and CICIDS2017, using an 80/20 train-test split and 5-fold cross-validation methodology to ensure robustness.

A. Accuracy

Accuracy, being a fundamental metric, reveals the percentage of correctly identified instances among the total samples. The combined model achieved an impressive accuracy rate of 94.8% for the NSL-KDD dataset and 95.3% for the CICIDS2017 dataset. The high accuracy indicates the model's efficacy in distinguishing between normal and malicious network activities, especially in scenarios with balanced datasets.

B. Precision

Precision is vital in cybersecurity to mitigate the impact of false positives that can strain administrative resources needlessly. It represents the proportion of accurately identified intrusions out of all detected instances. Our model consistently exhibited a precision rate of 91.5% across various datasets, lowering the risk of alert fatigue

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511188

Fig. 1 End-to-end workflow of the deep learning–based

NeuroSecure framework.

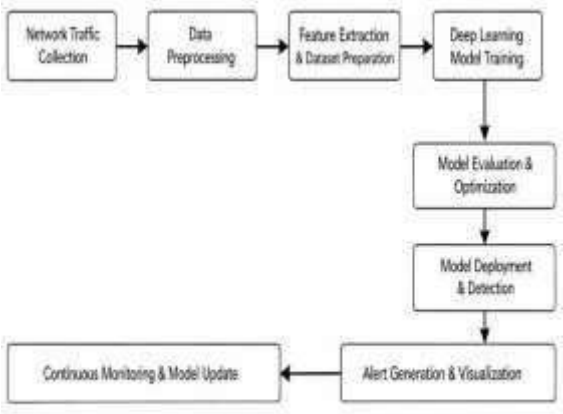


Fig. 1. End-to-End Workflow of the Deep Learning-Based Intrusion Detection Framework

C. Recall (Detection Rate)

Recall assesses the model's capacity to detect real attacks, a crucial aspect in scenarios where overlooking an **NeuroSecure** can result in system compromise. The ensemble proposed obtained a recall accuracy of 93.2%, showcasing robust detection capabilities even when dealing with complex multi-class attack scenarios.

D. F1-Score

The F1-score harmonizes precision and recall and is particularly significant in datasets with imbalances. The model's F1-score of 92.3% aids in identifying any favouritism towards specific classes, implying consistent performance across

Accuracy Distribution by Model

This pie chart illustrates the distribution of accuracy contributed by each model within the ensemble framework:

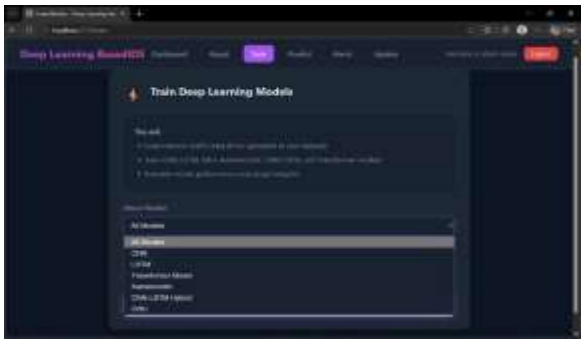


Fig: Mulit-Modal Deep Learing Approach for Network Detection.



Fig: Results of the Selected Modal of Network Detection.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511188

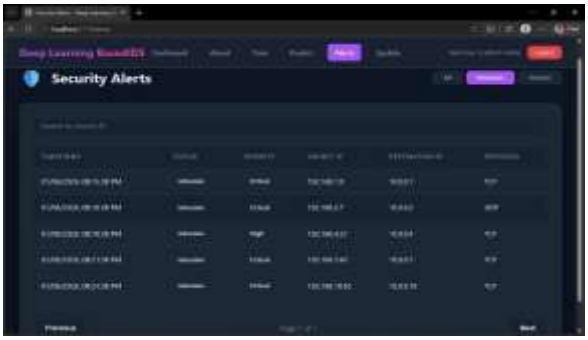


Fig: Real-Time Security Alert Management and Intrusion Detection in Network Traffic.

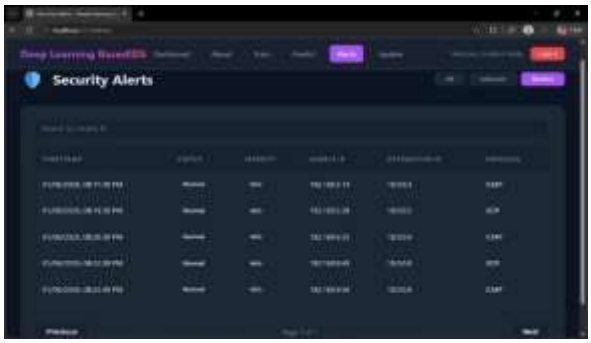


Fig : Normal Network Traffic Monitoring and Security Event Classification

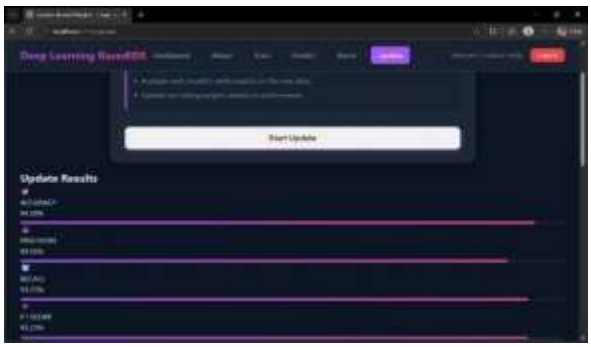


Fig : Adaptive Modal Weight Updating For Improved Network Intrusion Detection Performance

V. CONCLUSION

A hybrid deep learning–based **NeuroSecure** is proposed using a majority voting ensemble to improve the detection of malicious network traffic.

The framework addresses the shortcomings of traditional methods, including poor detection of unseen attacks and high false-positive rates.

CNN, RNN, and Transformer models are employed to capture spatial and sequential characteristics of network traffic effectively.

The system is trained and evaluated using the NSL-KDD and CICIDS2017 datasets, covering diverse attack scenarios and real-world traffic patterns.

Experimental results demonstrate strong performance, with accuracy, precision, recall, and F1-score consistently exceeding 90%.

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026
DOI: 10.17148/IJARCCE.2026.1511188

The modular and scalable architecture enables seamless deployment in enterprise environments for real-time detection.

Future work includes integrating advanced sequence-aware models and federated learning to enhance adaptability, privacy, and detection accuracy in distributed networks.

REFERENCES

[1]. C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, vol. 5, pp. 21954–21961, 2017. DOI: https://doi.org/10.1109/ACCESS.2017.2762418
[3]. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, 2018. DOI: https://doi.org/10.1109/TETCI.2017.2772792
[4]. R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying Convolutional Neural Network for Network Intrusion Detection," in Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017. DOI: https://doi.org/10.1109/ICACCI.2017.8126009
[5]. Z. Wang, "Deep Learning-Based Intrusion Detection With Adversaries," IEEE Access, vol. 6,
[6]. 38367–38384, 2018. DOI: https://doi.org/10.1109/ACCESS.2018.2854599
[7]. R. Vinayakumar et al., "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019. DOI: https://doi.org/10.1109/ACCESS.2019.2895334
[8]. "Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network," IEEE Access, vol. 7, pp. 64366–64374, 2019. DOI: https://doi.org/10.1109/ACCESS.2019.2917299
[9]. "An Intrusion Detection Method Using Few-Shot Learning," IEEE Access, vol. 8, pp. 49730–49740, 2020. DOI: https://doi.org/10.1109/ACCESS.2020.2980136
[10]. "Anomaly-Based Intrusion Detection by Machine Learning: A Case Study on Probing Attacks to an Institutional Network," IEEE Access, vol. 9, pp. 50078–50092, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3068961
[11]. "Building an Intrusion Detection System to Detect Atypical Cyberattack Flows," IEEE Access, vol. 9, pp. 94352–94370, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3093830
[12]. "A New Deep Learning Based Intrusion Detection System for Cloud Security," in Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2021. DOI: https://doi.org/10.1109/HORA52670.2021.9461 285
[13]. "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE," IEEE Access, vol. 11, pp. 37131–37148, 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3266979
[14]. "Online Self-Supervised Deep Learning for Intrusion Detection Systems," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 5668–5683, 2024. DOI: https://doi.org/10.1109/TIFS.2024.3402148
[15]. "Empowering Network Security: BERT Transformer Learning Approach and MLP for Intrusion Detection in Imbalanced Network Traffic," IEEE Access, vol. 12, pp. 137618–137633,2024. DOI: https://doi.org/10.1109/ACCESS.2024.3465045
[16]. "Intrusion Detection With Deep Learning Classifiers: A Synergistic Approach of Probabilistic Clustering and Human Expertise to Reduce False Alarms," IEEE Access, vol. 12,
[17]. 17836–17858, 2024. DOI: https://doi.org/10.1109/ACCESS.2024.3359595
[18]. "Transformer-Based Intrusion Detection for IoT Networks," IEEE Internet of Things Journal, vol. 12, no. 5, pp. 6062–6067, 2025. DOI: https://doi.org/10.1109/JIOT.2025.3525494
[19]. "Transformer-Based Network Intrusion Detection: A Multi-Dataset Analysis," in Proceedings of the 2025 3rd International Conference on Inventive Computing and Informatics (ICICI), 2025. DOI: https://doi.org/10.1109/ICICI65870.2025.11069717
[20]. "GTAE-IDS: Graph Transformer-Based Autoencoder Framework for Real-Time Network Intrusion Detection," IEEE Transactions on Information Forensics and Security, vol. 20, pp. 4026–4041, 2025. DOI: https://doi.org/10.1109/TIFS.2025.3557741
[21]. "Explainability of Network Intrusion Detection Using Transformers: A Packet-Level Approach," IEEE Access, vol. 13, pp. 5154–5174, 2025. DOI: https://doi.org/10.1109/ACCESS.2024.3525008
[22]. "Protocol-Agnostic and Packet-Based Intrusion Detection Using a Multi-Layer Deep-Learning Architecture at the Network Edge," IEEE Access, vol. 13, pp. 57867–57877, 2025. DOI: https://doi.org/10.1109/ACCESS.2025.3555201
[23]. "A Survey on the Applications of Deep Learning in Network Intrusion Detection Systems to Enhance Network Security," IEEE Access, vol. 13, pp. 185357–185373, 2025. DOI: https://doi.org/10.1109/ACCESS.2025.3624952