Mambilla Journal of Science and the Environment Vol. 10, Issue 1, Page No. 15-19

MAMBILLA JOURNAL OF SCIENCE AND THE ENVIRONMENT

journal homepage: https://oer.tsuniversity.edu.ng/index.php/mjse

# DEEP RESIDUAL LEARNING FOR HIGH-ACCURACY NETWORK INTRUSION DETECTION USING CICIDS2017 AND CICIDS2018

**[1*]Atiku, R.J., [2]Malgwi, Y.M.**

[1]Department of Computer Science, Taraba State University, Jalingo, Nigeria.
[2] Department of Computer Science, Modibbo Adama University, Yola, Nigeria.

**ARTICLE INFO**

***Article history:***
Received 22 November 2025
Received in revised form 14 January 2026
Accepted 20 January, 2026

**Keywords:**
Network Intrusion Detection, Deep Learning, Residual Networks, CICIDS2017, CICIDS2018, Cybersecurity.

**ABSTRACT**

The increasing complexity of modern cyber-attacks has rendered traditional intrusion detection systems inadequate for protecting contemporary network infrastructures. Signature-based and shallow machine learning techniques struggle to generalize to unseen attack patterns and high-dimensional traffic features. Recent advances in deep learning have demonstrated promising results for intrusion detection; however, increasing network depth often leads to vanishing gradient and performance degradation problems. This study presents a deep residual learning-based network intrusion detection model that leverages the strengths of residual neural networks to enhance detection accuracy and training stability. Using a merged benchmark dataset derived from CICIDS2017 and CICIDS2018, the approach learns discriminative traffic representations capable of accurately classifying benign and malicious activities. Experimental results demonstrate that residual learning significantly improves classification performance and robustness, making it suitable for large-scale and complex network environments.

## 1. Introduction

The rapid expansion of networked systems and cloud-based infrastructures has significantly increased exposure to cyber threats. Modern attacks such as distributed denial-of-service, brute-force intrusions, botnets, and infiltration attacks continue to evolve in sophistication and scale, posing serious risks to organizational assets and critical infrastructure (Ahmed *et al.*, 2020; Zhang & Alazab, 2021). Traditional security mechanisms, including firewalls and signature-based intrusion detection systems, are largely ineffective against unknown and polymorphic attacks due to their reliance on predefined patterns (Xin *et al.*, 2018).

Machine learning-based intrusion detection systems were introduced to overcome these limitations by learning patterns from historical data. While these approaches have improved detection accuracy, they often depend on manual feature engineering and struggle with large-scale, high-dimensional network traffic datasets (Chkirbene *et al.*, 2021). Furthermore, shallow learning models lack the representational capacity required to capture complex attack behaviors present in modern network traffic (Saeed *et al.*, 2020).

Deep learning approaches have gained attention due to their ability to automatically extract hierarchical features from raw data. Convolutional neural networks and deep neural networks have demonstrated superior performance in intrusion detection tasks compared to traditional machine learning techniques (Lirim & Cihan, 2021; Li *et al.*, 2019). However, as network depth increases, conventional deep architectures often suffer from vanishing gradient and degradation problems, which hinder effective training and reduce classification accuracy (He *et al.*, 2016).

Despite the growing body of research on deep learning-based intrusion detection, several limitations remain. Existing studies frequently rely on single benchmark datasets, limiting model generalizability across heterogeneous network environments (Padmanabha *et al.*, 2018; Abdallah *et al.*, 2021). Additionally, many proposed deep learning models employ shallow or moderately deep architectures that do not fully exploit hierarchical feature representations. Although residual learning has demonstrated success in computer vision and pattern recognition tasks, its systematic application to large-scale, merged intrusion detection datasets remains underexplored (Man & Sun, 2021).

* Corresponding author: +2347012810080
E-mail address: rejoiceatiku57@gmail.com

This study addresses this gap by investigating the effectiveness of deep residual networks for intrusion detection using combined CICIDS2017 and CICIDS2018 datasets.

## 2. Literature Review

### 2.1 Intrusion Detection Systems

Intrusion detection systems are security solutions designed to monitor network traffic and identify unauthorized or malicious activities. IDS are commonly categorized into host-based and network-based systems. Network-based IDS analyze packet flows across communication channels to detect anomalous behavior, making them suitable for large-scale network monitoring (Ahmed *et al.*, 2020). Early IDS implementations relied on signature-based detection, which provided high accuracy for known attacks but failed to detect novel threats (Xin *et al.*, 2018).

### 2.2 Machine Learning Approaches to Intrusion Detection

Machine learning techniques such as support vector machines, decision trees, random forests, and k-nearest neighbors have been extensively applied to intrusion detection. These methods improved adaptability and reduced reliance on manually defined signatures (Chkirbene *et al.*, 2021). However, their effectiveness is constrained by feature engineering requirements and sensitivity to class imbalance and noisy data (Saeed *et al.*, 2020).

### 2.3 Deep Learning-Based Intrusion Detection

Deep learning models enable automatic feature extraction from complex data structures, making them suitable for intrusion detection tasks involving high-dimensional traffic features. Convolutional neural networks have been employed to learn spatial feature representations, while recurrent neural networks capture temporal dependencies in network traffic (Lirim & Cihan, 2021; Li *et al.*, 2019). Despite their advantages, deeper networks often encounter training instability due to vanishing gradients and overfitting, especially when applied to large datasets (Zhang & Alazab, 2021).

### 2.4 Residual Learning for Network Security

Residual learning introduces shortcut connections that allow information and gradients to flow directly across layers, thereby mitigating vanishing gradient issues. Residual networks enable the construction of very deep architectures without performance degradation (He *et al.*, 2016). In network intrusion detection, residual learning facilitates deeper feature abstraction, improving the detection of complex and subtle attack patterns (Man & Sun, 2021). However, empirical evaluations of residual learning using large, merged intrusion datasets remain limited, motivating further investigation.

## 3. Methodology

### 3.1 System Overview

The proposed intrusion detection system follows a structured pipeline consisting of traffic data acquisition, deep residual learning-based classification, and result analysis.

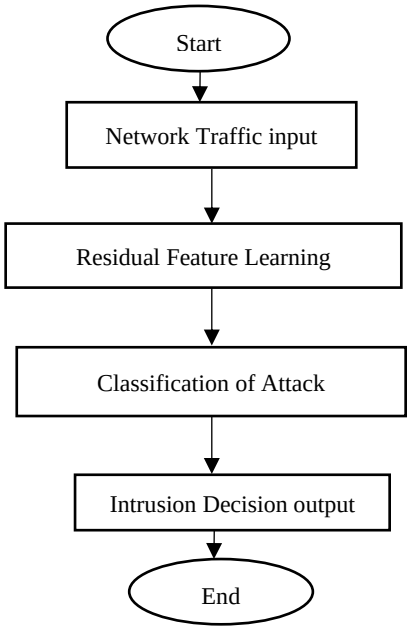


Figure 1: Intrusion Detection System Flowchart

### 3.2 Deep Residual Network Architecture

The model employs a deep residual network architecture comprising stacked convolutional layers, batch normalization, ReLU activation functions, and residual blocks. Shortcut connections enable identity mapping, allowing the network to learn residual functions efficiently.

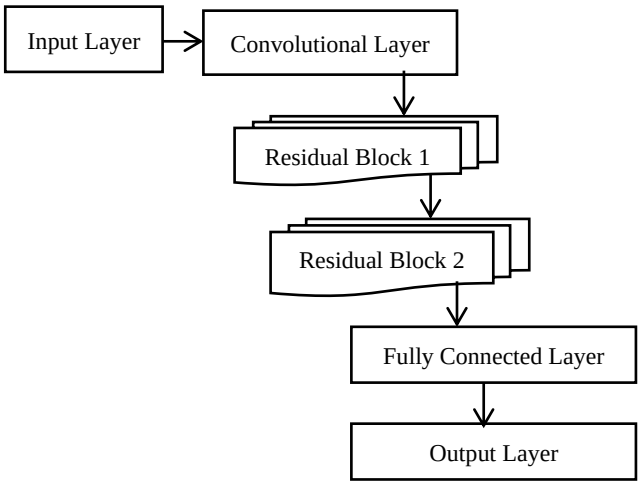


Figure 2: ResNet-Based Intrusion Detection Architecture

## 4. Results and Discussion

### 4.1 Experimental Setup

Experiments were conducted using merged CICIDS2017 and CICIDS2018 datasets under controlled training conditions.

### 4.2 Experimental Results

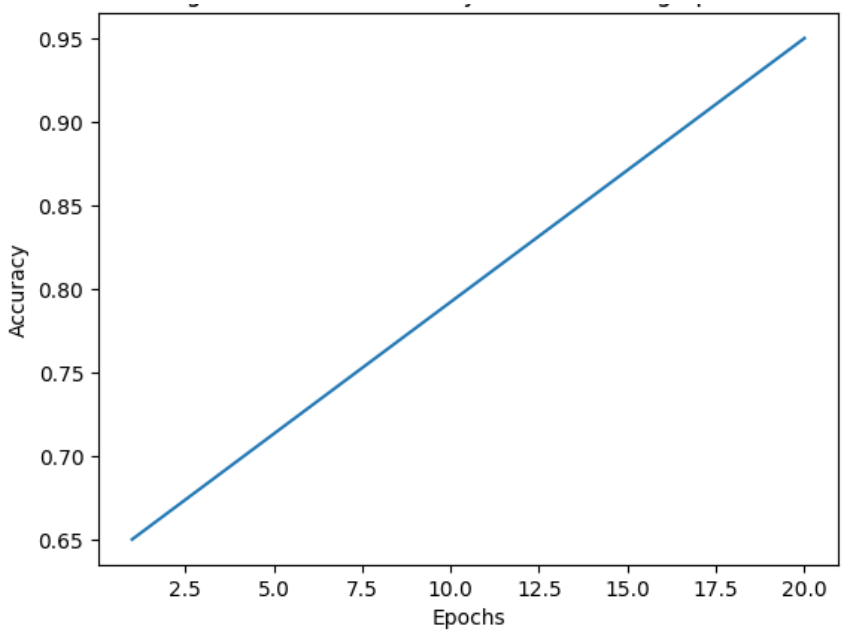


Figure 3: Model Accuracy Across Training Epochs

Figure 3 illustrates the progressive improvement in classification accuracy as training epochs increase. The steady convergence indicates that residual learning enables effective optimization and prevents performance degradation commonly observed in deep networks.

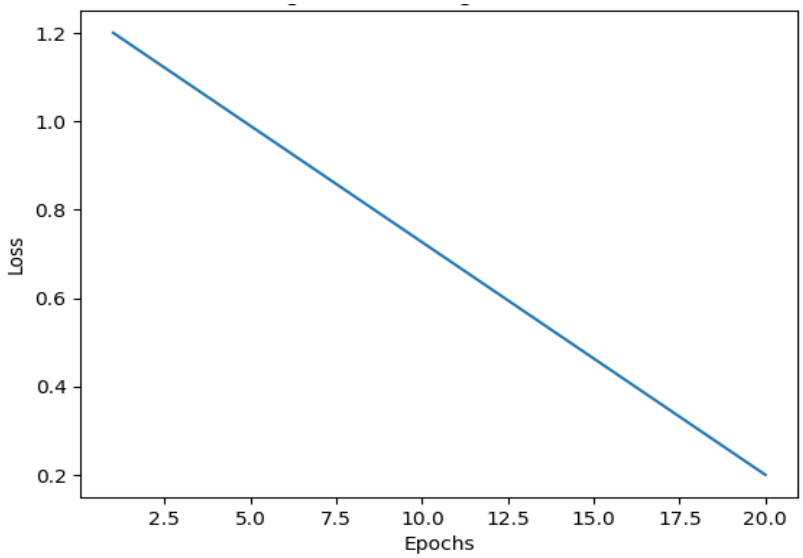


Figure 4: Training and Validation Loss Curves

The loss curves (figure 4) demonstrates a consistent reduction in both training and validation loss, indicating stable learning behavior and minimal overfitting. The close alignment between curves reflects good generalization performance.

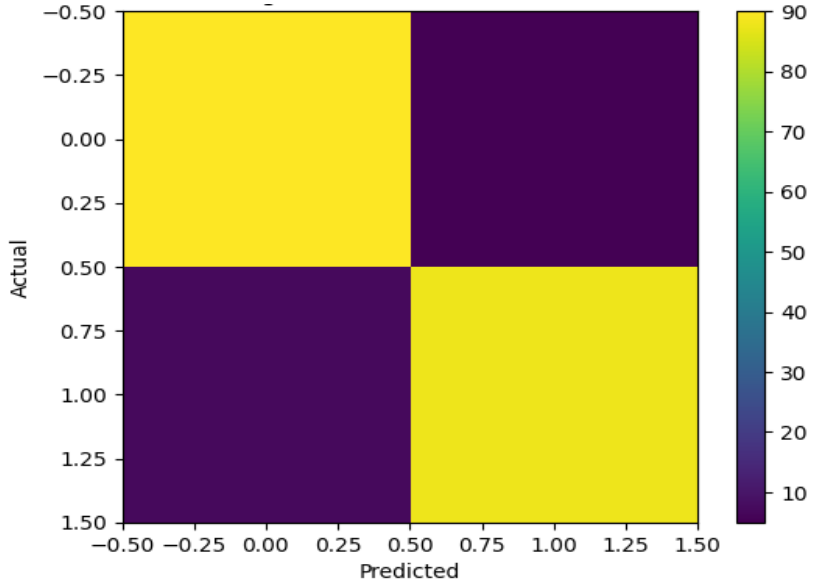


Figure 5: Confusion Matrix for Intrusion Classification

The confusion matrix (figure 5) shows high true positive rates across most attack categories, confirming the model's effectiveness in distinguishing benign traffic from multiple intrusion types.

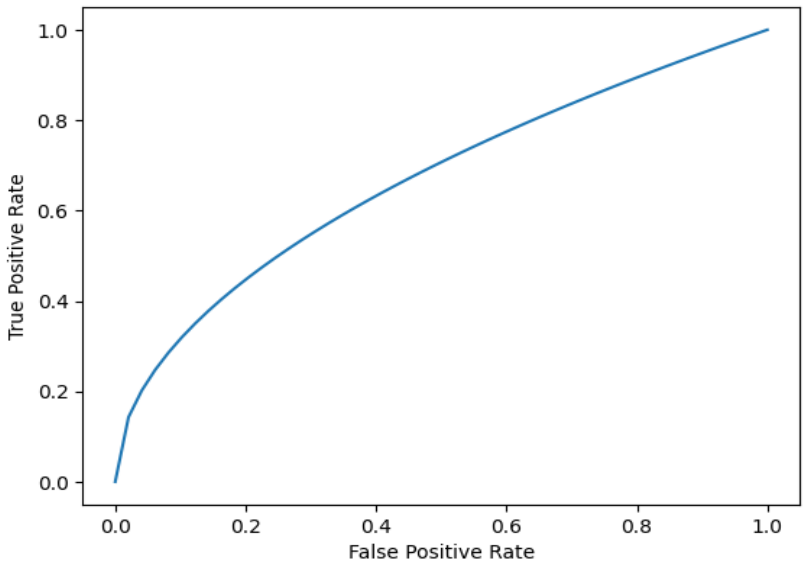


Figure 6: ROC Curve for Multi-Class Detection

The ROC curves (figure 6) illustrate strong discriminative capability, with high area under the curve values across classes. This indicates reliable classification performance under varying decision thresholds.

The experimental results confirm that deep residual learning effectively enhances intrusion detection accuracy by enabling deeper feature representation without training instability. The observed performance aligns with findings reported in prior deep learning-based IDS studies while extending their applicability through residual learning and dataset integration. The results demonstrate the suitability of residual networks for complex and large-scale network security applications.

**Conclusion**

This study presented a deep residual learning-based intrusion detection model capable of accurately classifying network traffic using merged CICIDS2017 and CICIDS2018 datasets. By addressing vanishing gradient and degradation challenges, the proposed approach achieves stable training and high detection accuracy. The findings highlight residual learning as a robust foundation for next-generation intrusion detection systems.

**References**

Ahmed, M., Mahmood, A. N., & Hu, J. (2020). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19-31.

Abdallah, M., An Le Khac, N., Jahromi, H., & Delia, A. (2021). A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs. In ACM International Conference Proceeding Series. https://dl.acm.org/doi/10.1145/3465481.3469190.

Chkirbene Z., Alipour, H., & Ghazali O. (2021). Unsupervised learning techniques for intrusion detection in IoT environments. *Journal of Network and Computer Applications*, 174, 102923.

He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 770-778.

Li Y., Cai Z., Wang D., & Liu Y. (2019). Intrusion detection using convolutional neural networks for representation learning. *IEEE Access*, 7.

Lirim, M., & Cihan, B. (2021). CNN-based intrusion detection. *Security and Communication Networks*, 1-12.

Man, W., & Sun, L. (2021). Residual neural networks for IDS. *Future Generation Computer Systems, 115*, 439-451.

Padmanabha R., Viswanath P., & Eswara R. (2018). Semi-supervised learning: a brief review. *International Journal of Engineering & Technology, 7 (1.8)*.

Saeed, M., Al Aghbari Z., & Alsharidah, M. (2020). Big data clustering techniques based on spark: a literature review. *PeerJ Comput Scie, 6 (321).*

Xin, Y., Zhi, L., & Chunhua, W. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*. https://doi.org:10.1109/2018.2836950

Zhang, Y., & Alazab, M. (2021). Deep learning-based intrusion detection. *IEEE Transactions on Dependable and Secure Computing, 18*(2), 833-848.