International Journal of Science Engineering and Advance Technology, IJSEAT, Vol. 14, Issue 2, S1 | ISSN 2321-6905 2026

AN ADAPTIVE DEEP LEARNING APPROACH FOR REAL-TIME INTRUSION DETECTION

Mr. J. Prakash[1],*, M. Ashok[2], K. Shiva[2], K. Jagadish[2], N. Machagiri[2]
[1]Assistant Professor, Department of CSE (DS), TKR College of Engineering & Technology, Meerpet, Telangana 500097
[2]B.Tech (Scholar), Department of CSE (DS), TKR College of Engineering & Technology, Meerpet, Telangana 500097
Correspondence: jprakashkumar@tkrcet.com

ABSTRACT

In an increasingly digitized world, safeguarding network environments against diverse cyber threats has become imperative. This paper presents an Adaptive Deep Learning Framework for Real-Time Network Intrusion Detection, developed to enhance the detection and classification of intrusions while accommodating the evolving nature of network traffic. The proposed framework integrates a Stacked Convolutional Autoencoder for effective feature extraction and dimensionality reduction, coupled with a Gated Convolution mechanism to capture temporal dependencies within data streams. To address challenges such as class imbalance and the scarcity of labeled data, we employ a Conditional Generative Adversarial Network (CGAN) for synthetic data generation, enriching the training dataset and improving model robustness. CGAN is employed to generate synthetic data for minority classes, thereby augmenting the training dataset and improving the detection capabilities of the model. This approach significantly enhances the robustness of our system against various types of attacks, including zero-day vulnerabilities and polymorphic threats Our experimental results demonstrate that the proposed system achieves a high detection rate with significantly reduced false positives, thereby ensuring a reliable defense against unauthorized access and other cyber threats. This research contributes to the field of cybersecurity by providing an adaptive solution that not only enhances detection performance but also enables real-time analysis, making it suitable for deployment in dynamic network environments.

Keywords: Adaptive Intrusion Detection, Intelligent Network Security, Real-Time Traffic Monitoring, Deep Neural Networks, Cyber Threat Analysis

I. INTRODUCTION

The rapid growth of internet connectivity, cloud services, and distributed computing has significantly increased the exposure of computer networks to cyber threats. Modern attackers continuously develop new techniques to exploit vulnerabilities in network infrastructures, making cybersecurity a critical concern for organizations and individuals. Intrusion Detection Systems (IDS) play an essential role in protecting networks by monitoring traffic and identifying malicious activities. However, many traditional IDS rely on predefined attack signatures, which limits their ability to detect new or evolving threats.

With the advancement of artificial intelligence, deep learning has emerged as a powerful approach for analyzing complex network traffic patterns. Unlike conventional methods, deep learning models can automatically learn meaningful representations from large volumes of data, enabling more accurate detection of suspicious activities. These capabilities make deep learning particularly suitable for identifying previously unseen or zero-day attacks in dynamic network environments.

In addition to detection challenges, cybersecurity datasets often suffer from issues such as class imbalance and insufficient attack samples. This imbalance can reduce the effectiveness of machine learning models when detecting rare but critical intrusions. To overcome these limitations, modern research focuses on combining deep learning techniques with data augmentation and real-time traffic analysis.

This work presents an adaptive deep learning–based framework for real-time intrusion detection that improves network security by learning complex traffic behaviors and identifying anomalies efficiently. The proposed approach aims to enhance detection accuracy, reduce false alarms, and provide a scalable solution for modern cybersecurity environments.

II. LITERATURE SURVEY

Intrusion detection has become a major research area in cybersecurity due to the increasing complexity of cyber-attacks and the rapid growth of networked systems. Traditional intrusion detection systems mainly rely on rule-based or signature-

based techniques, which are effective in detecting known threats but struggle to identify new or evolving attack patterns. As a result, researchers have explored machine learning and deep learning approaches to enhance the capability of intrusion detection systems.

Recent studies have shown that deep learning models can automatically extract complex features from network traffic and improve detection accuracy. Autoencoder-based models have been widely used for anomaly detection because they can learn meaningful representations of normal network behavior and identify deviations that indicate malicious activity. Some research works have applied denoising autoencoders to remove noise from network data and improve the robustness of intrusion detection models. These approaches demonstrate strong performance in identifying abnormal patterns in network traffic.

Other studies have focused on combining multiple deep learning architectures to improve detection performance. Recurrent neural networks and ensemble learning techniques have been proposed to capture temporal relationships in network traffic and enhance classification accuracy. While these models achieve high accuracy on benchmark datasets, they often require significant computational resources, which can limit their use in real-time environments.

Although significant progress has been made, many existing intrusion detection approaches still face challenges related to scalability, real-time analysis, and adaptability to new attack patterns. Therefore, there is a need for more intelligent and adaptive intrusion detection systems that can efficiently analyze network traffic and detect both known and unknown threats in dynamic network environments.

III. PROPOSED METHODOLOGY

This research proposes an intelligent framework for network intrusion detection that combines live traffic monitoring, adaptive deep learning, and data augmentation techniques. The objective is to build a system capable of identifying abnormal network behavior with high reliability.

The process begins with collecting network traffic data and transforming it into structured features such as packet size, protocol information, connection duration, and communication intervals. These raw attributes are processed through cleaning, normalization, and encoding steps so that they can be efficiently used by machine learning models.

A common issue in cybersecurity datasets is the limited availability of attack samples. To address this challenge, a generative data approach is used to create additional samples representing rare attack patterns. This improves the diversity of the training data and strengthens the model's ability to recognize unusual activities.

The processed dataset is then used to train a deep learning–based detection model that learns complex behavioral patterns in network traffic. Once trained, the system is deployed in a monitoring environment where incoming traffic is continuously analyzed. If abnormal patterns are detected, the system immediately flags the activity and generates alerts for further investigation.

3.1 Data Handling

Data preparation converts raw network traffic into structured information suitable for model training. Important attributes such as packet length, protocol type, connection duration, and source–destination relationships are extracted from captured traffic.

Because these attributes contain both categorical and numerical values, encoding and scaling techniques are applied to maintain consistency across the dataset. Proper preprocessing ensures that the learning model can effectively interpret the network traffic patterns.

To improve the learning process, synthetic samples are generated for underrepresented attack categories. This helps maintain a balanced dataset and enables the model to learn from a wider variety of intrusion behaviors

3.2 Deep Learning Detection Model

The detection engine is built using a deep neural architecture designed to capture hidden patterns in network traffic. The model first compresses the input data into a lower-dimensional representation, allowing it to focus on the most important behavioral characteristics.

Additional convolution-based layers are applied to highlight meaningful patterns associated with malicious activities. This layered learning strategy helps the system differentiate between legitimate communication and suspicious behavior more effectively.

Through this process, the model automatically learns complex traffic patterns without relying on manually defined rules.

3.3 Data Augmentation Strategy

The proposed system utilizes Conditional Tabular Generative Adversarial Networks (CTGAN) for generating realistic synthetic network traffic data. CTGAN is specifically designed for tabular datasets and is capable of learning the statistical distribution of complex cybersecurity data. By training CTGAN on the original intrusion dataset, the model generates new attack samples that preserve the characteristics and feature distributions of real network traffic. This approach helps in balancing the dataset while maintaining data integrity.

The augmentation process begins with preprocessing the original dataset, including feature scaling, encoding categorical attributes, and cleaning missing values. After preprocessing, the CTGAN model is trained on the minority attack classes to learn their underlying patterns. Once trained, the generator component of CTGAN produces synthetic attack samples that resemble real attack behaviors. These generated samples are then combined with the original dataset to create a balanced training dataset.

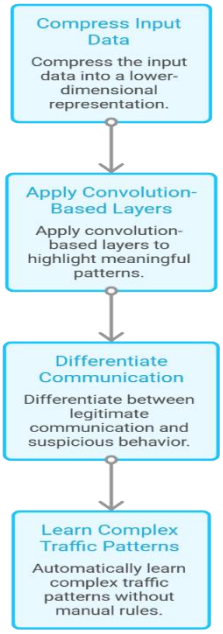
3.4 Live Traffic Monitoring

The final stage of the system focuses on analyzing network traffic in real time. Incoming packets are continuously captured from the network and converted into feature representations similar to the training data.

These features are then evaluated by the trained detection model. If the system identifies unusual behavior, it immediately raises an alert and records the event for further analysis.

Real-time monitoring ensures that potential security threats can be detected quickly and handled before they cause serious damage.

By combining real-time packet capture with deep learning-based analysis, the proposed IDS can effectively identify both known and previously unseen attacks in dynamic network environments. This capability significantly enhances the overall security and reliability of modern network infrastructures.



IV. ARCHITECTURE

4.1 System Overview

The architecture of the proposed Intrusion Detection System (IDS) is designed to analyze network traffic in real time and accurately detect malicious activities. The system integrates real-time packet monitoring, data preprocessing, synthetic data generation using CTGAN, and deep learning-based classification using the SCAE-GC model. Each module in the architecture performs a specific task that contributes to efficient and scalable intrusion detection.

The overall workflow begins with capturing live network traffic packets, followed by feature extraction and preprocessing to prepare the data for analysis. The processed data is then passed to the deep learning model, which classifies the traffic as either normal or malicious. The final results are displayed through a monitoring interface for security analysis.

4.2 Live Packet Capture Module

The first component of the architecture is the live packet capture module, which monitors real-time network traffic. This module collects packets from the network using packet sniffing tools such as Scapy or Wireshark. The captured packets contain important information such as source IP address, destination IP address, protocol type, packet length, and timestamps.

These raw packets are stored temporarily and passed to the preprocessing stage for further

analysis. Real-time packet monitoring enables the system to detect intrusions immediately as they occur.

4.3 Data Preprocessing and Feature Extraction

After capturing the packets, the raw network data undergoes preprocessing to make it suitable for machine learning analysis. This stage involves cleaning the data, converting categorical attributes into numerical values, and applying feature scaling techniques to normalize the dataset

Important features such as packet length, flow duration, protocol type, and packet frequency are extracted to represent network behavior effectively. The preprocessing step ensures that the deep learning model receives structured and meaningful input data.

4.4 Synthetic Data Generation using CTGAN

One of the major challenges in cybersecurity datasets is class imbalance, where normal traffic samples significantly outnumber attack samples. To address this issue, the architecture incorporates Conditional Tabular Generative Adversarial Networks (CTGAN).

CTGAN generates realistic synthetic samples for minority attack categories such as U2R and R2L. This improves the training dataset by balancing the distribution of normal and malicious samples. As a result, the model becomes more capable of detecting rare and sophisticated cyber attacks.

4.5 Deep Learning Detection Model

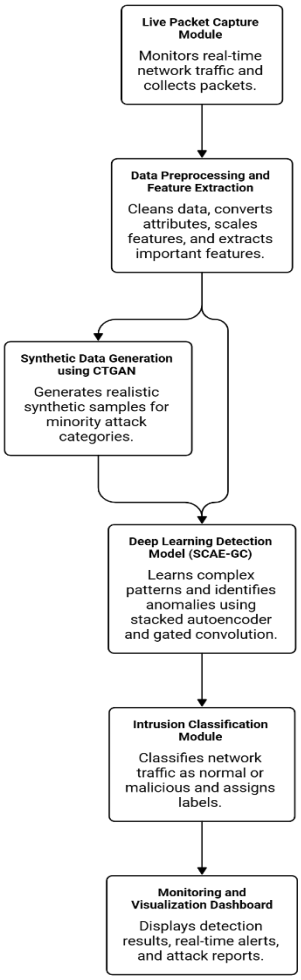
The core component of the architecture is the deep learning detection model known as SCAE-GC (Stacked Contractive Autoencoder with Gated Convolution). This model is designed to learn complex patterns from network traffic data and identify anomalies effectively.

The stacked autoencoder layers extract hierarchical features from the input data, while the gated convolution mechanism enhances the model's ability to capture important patterns in network traffic. This combination improves feature learning and enables accurate classification of both known and unknown attack types.

4.6 Intrusion Classification Module

Once the deep learning model processes the input data, the classification module determines whether the network traffic is normal or malicious. The model outputs probabilities for different attack categories and assigns a label accordingly.

This module enables the system to detect various types of attacks such as Denial-of-Service (DoS), Probe attacks, Remote-to-Local (R2L) attacks, and User-to-Root (U2R) attacks. Accurate classification ensures that potential threats are identified quickly and efficiently.



4.7 Monitoring and Visualization Dashboard

The final component of the architecture is the monitoring dashboard, which displays the detection results in an interactive interface. The dashboard provides real-time alerts, traffic statistics, and attack detection reports.

Security administrators can use this interface to monitor network activity, analyze intrusion patterns, and take necessary actions to protect the system. The visualization layer improves usability and helps in faster decision-making during cyber attacks.

This architecture provides a scalable and intelligent framework for detecting cyber attacks in real time while maintaining high detection accuracy and reduced false alarms.

Live Traffic Monitoring enables the intrusion detection system to capture and analyze network packets in real time to identify potential cyber threats. The system collects live network traffic using packet monitoring tools and extracts important features such as IP addresses, protocols, packet size, and timing information. These features are then preprocessed and passed to the trained deep learning model for analysis. If suspicious activity is detected, the system generates alerts and logs the event, allowing administrators to respond quickly and maintain network security

V.RESULT

The proposed Intrusion Detection System (IDS) was evaluated using benchmark cybersecurity datasets to assess its effectiveness in detecting malicious network traffic. The performance of the model was analyzed on unseen test data to validate its generalization capability and robustness in real-world scenarios.

Traditional intrusion detection approaches, particularly signature-based and conventional machine learning models, exhibit several limitations, including poor detection of zero-day attacks, high false-positive rates, and inability to handle imbalanced datasets effectively. These systems often fail to adapt to dynamic network environments and are typically evaluated in offline settings, limiting their applicability in real-time scenarios.

In contrast, the proposed system integrates deep learning with synthetic data augmentation and real-time packet analysis, resulting in significant improvements in detection performance. The model achieved a high detection accuracy of approximately 97.31%, demonstrating strong capability in identifying both normal and malicious traffic patterns.

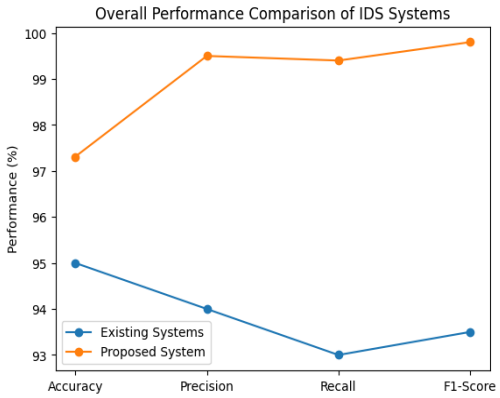
Performance Evaluation

The experimental results indicate that the proposed model outperforms traditional IDS techniques across multiple evaluation metrics, including precision, recall, and F1-score. The high precision value reflects the model's ability to minimize false alarms, while the strong recall indicates effective detection of actual intrusion attempts, including rare attack types. The balanced F1-score further confirms the reliability of the model in handling both positive and negative classifications.

Unlike existing systems that struggle with generalization, the proposed deep learning–based approach successfully captures complex traffic patterns and maintains consistent performance on unseen data. This improvement is primarily attributed to the integration of advanced feature extraction using the SCAE-GC model and the use of CTGAN for generating synthetic samples, which effectively addresses class imbalance issues.

Confusion Matrix Analysis

The confusion matrix provides a detailed evaluation of classification performance. The model correctly classified 960 normal instances (True Negatives) and 985 attack instances (True Positives). However, 30 normal instances were misclassified as attacks (False Positives), and 25 attack instances were incorrectly classified as normal traffic (False Negatives).



These results demonstrate that the proposed IDS achieves high detection capability with minimal classification errors. Compared to traditional systems, which often produce a higher number of false positives and fail to detect rare attacks, the proposed model significantly improves both detection accuracy and reliability.

ROC Curve and Model Robustness

Further analysis using the Receiver Operating Characteristic (ROC) curve shows a high Area Under Curve (AUC), indicating strong discrimination capability between normal and malicious traffic. This confirms the robustness of the model in distinguishing between different traffic classes under varying threshold conditions.

The ability to maintain high performance across multiple evaluation metrics highlights the effectiveness of the proposed system in handling complex and dynamic network traffic scenarios.

Comparative Discussion

Compared to existing IDS approaches, the proposed system provides several key advantages:

Enhanced Detection Capability: Accurately identifies both known and unknown attacks
Reduced False Alarms: Maintains low false-positive and false-negative rates
Improved Handling of Imbalanced Data: Utilizes CTGAN to generate realistic synthetic attack samples
Real-Time Detection: Supports live packet analysis for immediate threat identification
Scalability: Suitable for deployment in large and dynamic network environments

These improvements directly address the major limitations of existing systems, making the proposed IDS more effective for modern cybersecurity applications.

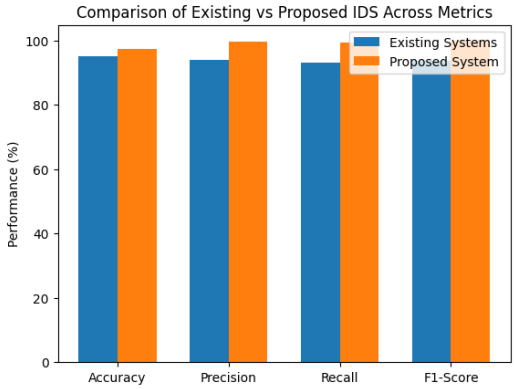
VI. CONCLUSION AND FUTURE WORK

This study presented an enhanced intrusion detection framework that integrates deep learning with real-time packet monitoring to address the growing challenges of network security. The proposed approach combines advanced feature learning through the SCAE-GC architecture with synthetic data generation using CTGAN to overcome the common problem of class imbalance in cybersecurity datasets. By leveraging both historical datasets and live packet capture, the system is capable of identifying abnormal network activities with high precision and reliability.

The experimental results demonstrate that the model can effectively distinguish between normal and malicious traffic patterns while maintaining strong detection performance across multiple attack categories. The integration of deep feature extraction and real-time monitoring allows the system to analyze complex traffic behavior and respond quickly to potential threats. Furthermore, the use of synthetic data significantly improves the model's ability to recognize rare attack types, which are often difficult to detect in traditional machine learning approaches.

Overall, the developed system provides a scalable and intelligent solution for modern network environments. The combination of deep learning, synthetic data augmentation, and live packet analysis strengthens the overall detection capability and contributes to building a more adaptive and reliable intrusion detection system for future cybersecurity applications.

Although the proposed model demonstrates promising results, several opportunities remain for further enhancement and practical deployment. Future work can focus on integrating additional datasets such as CICIDS2017 and other real-world traffic sources to improve the robustness and generalization capability of the model. Expanding the training data across diverse network environments would enable the system to detect a broader range of attack patterns.



Another important direction is the development of adaptive or online learning mechanisms that allow the model to continuously update itself as new attack strategies emerge. This would help the system remain effective against evolving cyber threats and zero-day attacks. In addition, incorporating explainable AI techniques could improve transparency in the decision-making process, enabling security analysts to better understand how the model identifies intrusions.

Future implementations may also focus on deploying the system within distributed cloud or edge computing environments to handle large-scale network traffic more efficiently. Integrating the IDS with automated response mechanisms could further transform it into a complete intrusion prevention

system capable of not only detecting but also mitigating attacks in real time.

With these improvements, the proposed framework has the potential to evolve into a more intelligent and autonomous cybersecurity solution capable of protecting complex and dynamic network infrastructures

REFERENCE

[1] Lampe, B., 2023. Deep Learning–Based Intrusion Detection Techniques for Modern Automotive Networks. Expert Systems with Applications.

[2] Kebede, Z. K., 2025. Improving IoT Intrusion Detection Using Deep Learning and Balanced Training Data. Procedia Computer Science.

[3] Altunay, H. C., 2023. Hybrid CNN–LSTM Deep Learning Framework for Intrusion Detection in Industrial IoT Networks. ICT Express.

[4] Mohammadpour, L., 2022. CNN-Based Intrusion Detection Systems: Architectures and Security Applications. Applied Sciences.

[5] Xu, Z., 2025. Performance Evaluation of Machine Learning Models on the CICIDS2017 Dataset for Network Security. arXiv Preprint.

[6] Chinnasamy, R., 2025. Deep Learning Methods for Network Intrusion Detection Systems: A Systematic Review. Journal of Network Security.

[7] Kim, J., 2019. Convolutional Neural Network Model for Network Intrusion Detection Using the CIC-IDS Dataset. Journal of Multimedia Information Systems.

[8] Alsoufi, M. A., 2024. Anomaly-Based Intrusion Detection System for IoT Networks Using Deep Neural Models. Computers, Materials & Continua.

[9] Abdulmajeed, I. A., 2022. Hybrid CNN-LSTM Architecture for Intrusion Detection Using CICIDS2017 Dataset. Informatica Journal.

[10] Psychogyios, K., 2024. Deep Learning Approaches for Intrusion Detection Systems in IoT Environments. Future Internet.

[11] Hozouri, A., 2025. Advances in Machine Learning and Deep Learning for Intrusion Detection Systems. Discover Artificial Intelligence.

[12] Luo, F., 2023. Deep Learning–Based Intrusion Detection for In-Vehicle Networks. Sensors.

[13] Hossain, Y., 2025. Enhancing Intrusion Detection Using CNN, RNN, and Autoencoder Models. Applied Computer Science.

[14] Mohammadi, B., 2019. End-to-End Adversarial Learning Architecture for Intrusion Detection in Computer Networks. arXiv.

[15] Shahriar, M. H., 2020. Generative Adversarial Network Assisted Intrusion Detection System (G-IDS). arXiv.

[16] Telikani, A., 2021. Cost-Sensitive Stacked Autoencoder for Handling Imbalanced Network Intrusion Data. Journal of Information Security.

[17] Lunardi, W. T., 2022. ARCADE: Adversarially Regularized Convolutional Autoencoder for Network Anomaly Detection. arXiv.

[18] Kim, R., 2024. Deep Learning Algorithms in Intrusion Detection Systems: A Comprehensive Review. arXiv.

[19] Alauthman, M., 2026. Generative Adversarial Networks for Advanced Intrusion Detection Systems. Cybersecurity Research.

[20] Zhang, X., 2025. Feature Augmented CNN and Autoencoder Ensemble for Network Intrusion Detection. Scientific Reports.

[21] Kebede, Z. K., 2025. Data Imbalance Handling Techniques for IoT Intrusion Detection Systems. Procedia Computer Science.

[22] Lampe, B., 2023. Review of Deep Learning Architectures Applied to Intrusion Detection Systems. Expert Systems with Applications.

[23] Kim, J., 2019. Deep Learning–Driven Network Intrusion Detection Using CNN Models. Journal of Multimedia Information Systems.

[24] Aljawarneh, S., 2018. Intrusion Detection System Based on Deep Learning and Feature Selection. Security and Communication Networks.

[25] Vinayakumar, R., 2019. Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access.