Grenze International Journal of Engineering and Technology, June Issue

Intelligent Real-Time Anomaly Detection and Autoblocking Framework for Server Security using Machine Learning

G. Sangeetha[1], M. Devika[2], N. Devipriya[3] and D. Dharani[4]
[1]Assistant Professor, Department of Computer Science and Engineering, SRM Valliammai Engineering College, Kattankulathur
[2-4]B.E Final Year Students, Department of Computer Science and Engineering, SRM Valliammai Engineering College, Kattankulathur

***Abstract*— Cybersecurity threats continue to escalate, leaving servers increasingly vulnerable to compromise and disruption. Once breached, recovery often demands direct intervention from IT or security teams, highlighting the limitations of traditional rule-based and signature-driven defense systems. These conventional approaches struggle to detect novel or evolving attacks. To address this gap, we propose an intelligent, automated, real-time anomaly detection and auto-blocking framework powered by machine learning. The system integrates Random Forest and Isolation Forest algorithms to analyze live network traffic, supported by Scapy for packet capture and manipulation. By continuously monitoring traffic, the framework identifies abnormal patterns and transitions seamlessly from detection to mitigation - blocking suspicious IPs, terminating compromised connections, and preventing further exploitation. Designed with scalability and low latency in mind, the framework adapts to dynamic environments, offering a resilient and autonomous solution for modern server security.**

***Keywords*— Cybersecurity, Intelligent Threat Detection, Machine Learning, Real-Time Packet Analysis, Random Forest, Isolation Forest, Intrusion Detection System (IDS), Automated Blocking, Zero- day Attacks, Firewall Automation, Network Traffic Monitoring.**

I. INTRODUCTION

The swift growth of internet-connected systems has resulted in a considerable rise in cyberattacks and unauthorized access incidents. As organizations increasingly depend on servers to store data, communicate, and complete transactions, they are more often than not a target for threats like distributed denial-of-service (DDoS), brute-force attempts, port scanning, malware injection, and SQL injection. Common intrusion detection systems (IDS) are generally signature- based in detection, and can only identify known threats based on 'previously' identified attack patterns.

As a result of changing threats that do not conform to recognized attack patterns. In light of this, researchers and industrial focused on developing intelligent adaptive systems which use machine learning to identify anomalies in network behavior.

Hybrid models of supervised and unsupervised learning such as random forest and isolation forest have returned results capable of detecting complex and high- dimensional traffic patterns with relative success.

Grenze ID: 01.GIJET.12.2.22
© Grenze Scientific Society, 2026

In addition, these models classifies traffic, in real-time, as normal or malicious making them more suitable for intrusion prevention systems.

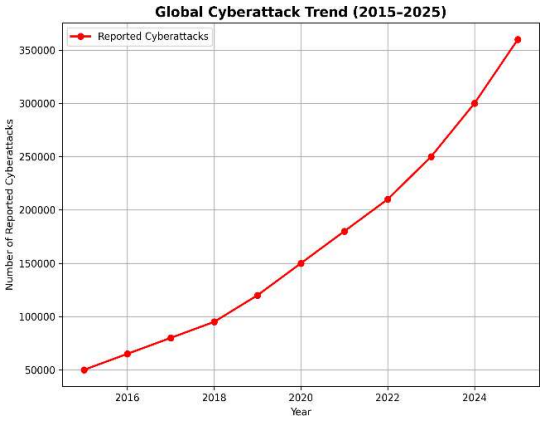

Fig. 1. Global cyberattack trend (2015-2025), motivating the need for intelligent intrusion detection systems

In this paper, we present a real-time detection of anomalous behavior and auto- blocking framework for increasing server security by analyzing live network traffic, tracking behavior anomalies, and automatic blocking of malicious network connections. In this approach, we utilize Scapy for packet captures, analyze captured traffic using a trained hybrid model, and then, in the event of an anomalous detection, contact the administrator with an alert and block the malicious connection(s).

Ironically, the result is a more secure server regardless of the standard server load.Hybrid models combining supervised and unsupervised learning such as random forest and isolation forest have shown promising results in detecting complex and high- dimensional traffic patterns. These models dynamically classify traffic as normal or malicious in real-time intrusion detection

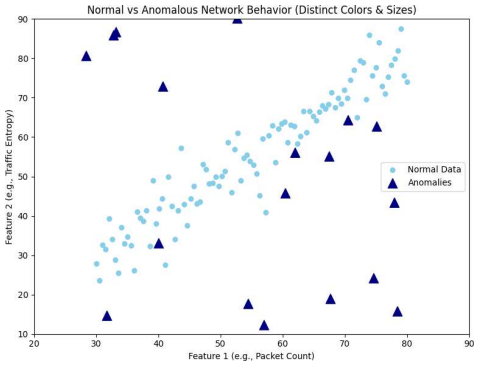

Fig. 2. Feature space visualization of network traffic, showing clear separation between normal and anomalous behavior.

This paper presents a real-time anomaly detection and auto-blocking framework that enhances server security by analyzing live network traffic, identifying threats, and automatically blockingmalicious connections.

The system uses Scapy for packet capture, processes data through a trained hybrid model, and triggers alerts and blocking mechanisms upon detecting anomalies. This approach ensures rapid response and minimizes the need for manual intervention, contributing to a more secure and resilient server infrastructure.

II. Literature Survey

Earlier intrusion detection systems mainly relied on rule-based and signature-based methods. While these methods were good at detecting known attack patterns, the reliance on predefined rules limited their performance when combating new or zero-day threats. In addition, as network environments changed, these systems struggled to adjust to increasingly dynamic traffic patterns and, therefore, their effectiveness dropped over time [5].

To address these limitations, researchers began to apply a variety of machine learning algorithms, including decision tree, support vector machine (SVM), and random forest models. These models were able to learn

patterns in the data to improve detection accuracy, and also provided a higher degree of intelligent detection of anomalies. However, they often suffered from issues surrounding class imbalance, false positives, and did not adapt in real-time [7].

Advanced frameworks, such as SAFE, proposed by Elvin Li et al., applied self-supervised learning and local outlier factor to detect zero-day attacks. Although these models were effective, they required a high amount of computer resource and introduced latency during periods of high traffic. Hybrid AI models combining deep learning and statistical learning, as suggested by Manoj Chowdary Vattikuti, were able to implement high precision models using off-the-shelf data, but were complex and computationally intensive.

Recent studies have explored hybrid approaches that integrate machine learning with deep learning to enhance detection capabilities. For example, Wang et al. proposed a hybrid intrusion detection system based on the combination of Random Forest and Autoencoder [1]. Similarly, Gill and Dhillon introduced a hybrid machine learning framework tailored for smart city environments, demonstrating improved adaptability and detection accuracy [2]. Almolhis further advanced hybrid IDS by combining Random Forest with attention mechanisms and explainable AI visualization [3]. Kumar and Patel extended this line of work by integrating Random Forest, Decision Tree, and ensemble learning for improved detection [4].

Other surveys have provided broad overviews of IDS design techniques, datasets, and network threats. Patcha and Park outlined anomaly detection techniques and their evolution [5], while Hindy et al. presented a taxonomy of IDS approaches and datasets [8]. These surveys highlight the growing complexity of IDS research and the need for hybrid and adaptive models.

Deep learning-based IDS approaches have also gained prominence. Kim provided a survey and performance comparison of deep learning IDS models [6]. Javaid et al. introduced one of the early deep learning approaches for IDS [11], while Meidan et al. developed N-BaIoT, a deep autoencoder-based IDS for IoT botnet detection [12]. Vinayakumar et al. proposed a comprehensive deep learning framework for intelligent IDS [13]. Liu et al. explored CNN and RNN-based methods for network intrusion detection [14], and Shone et al. demonstrated the use of stacked deep learning models for IDS [15].

Datasets remain critical for IDS evaluation. Tavallaee et al. provided a detailed analysis of the KDD CUP 99 dataset, which has been widely used in IDS research [10]. Zhang et al. applied isolation forest for anomaly detection in network traffic [9], showing its effectiveness in handling imbalanced data.

Lastly, other studies focused on addressing balance issues and reducing computer resource overhead. Studies by Faraz A. Khan and Lisong Shao proposed using resampling techniques and stacked autoencoders integrated with random forest models to improve detection of rare events. Omer Fawzi Awad's multi-algorithm method, which uses isolation forest and naive Bayes, enhanced scalability and reduced false negatives at the expense of considerable preprocessing. Qi Xie's sample equalization algorithm can effectively tackle class imbalance, but is less suited to dynamic traffic situations.

Taking this into account, the framework proposed here combines random forest and isolation forest to provide a real-time and adaptive IDS and auto-blocking system. The hybrid system guarantees fast detection and immediate response, and hence is applicable to contemporary server security.

IV. System Architecture and Methodology

The framework is composed of five important modules to allow for real-time detection, classification, and mitigation of threats occurring on the network. The framework obtains its capabilities through live traffic monitoring, machine learning-based analysis, and automated responses to threats detected to ultimately increase the security on the server.

A. Assumptions

The framework assumes the following conditions for deployment:

- The server operates under moderate to high traffic loads (up to 150 packets per second).
- Firewall rules are accessible for automated blocking of malicious IPs.
- Anomaly detection thresholds are empirically set at 0.7 to balance detection accuracy and false positives.
- The system is deployed in a Windows11 environment with Python 3.11, Scapy, and Scikit-learn libraries.

B. Data Acquisition and Scapy

Live packet capture is performed using Scapy, a Python-based tool for network packet analysis. Incoming and outgoing traffic is continuously monitored, and attributes such as IP addresses, protocol types, packet size, and timestamps are extracted for further processing.

C. Data Preprocessing and Feature Engineering

Captured packets undergo preprocessing to remove noise and normalize values. Key features include:

- Packet size and transmission rate
- Frequency of source and destination IPs
- Inter-arrival times
- Protocol usage and flag ratios

These features are scaled and encoded to improve model effectiveness and reduce false positives.

D. Model Training and Evaluation

Two complementary machine learning models are employed:

- Random Forest (RF): A supervised ensemble classifier trained on labeled datasets to distinguish malicious from normal traffic.
- Isolation Forest (IF): An unsupervised anomaly detection method that isolates rare or unknown threats by random feature selection and split points.

E. Real-Time Detection and Automatic Blocking

During deployment, each packet is examined in real time. If the anomaly score exceeds the threshold, firewall commands are executed to block the offending IP address. This prevents further communication from malicious sources and logs the event for administrator review.

F. Alert System for Administrators

Upon detection and blocking, the system generates alerts via email, SMS, or dashboard notifications. Each alert contains:

- Source IP and port
- Type of threat detected
- Timestamp of detection
- Action taken

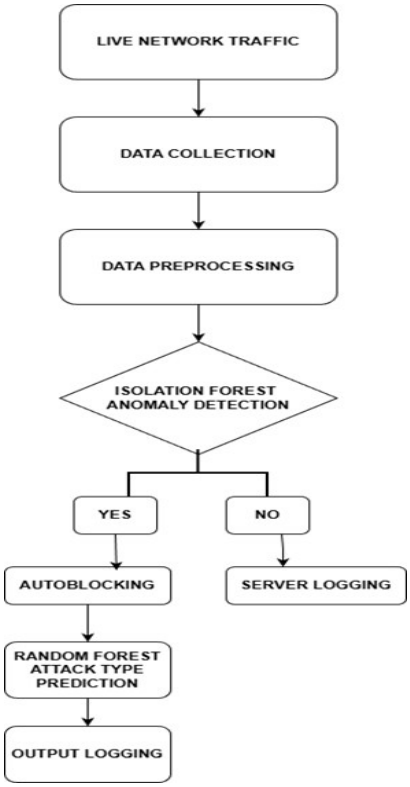

Fig. 3. System Architecture and Workflow of the Intelligent Real-Time Anomaly Detection and Auto- Blocking Framework

This ensures timely awareness and response by administrators without requiring constant supervision.
This modular workflow provides an end- to-end automated protection cycle, combining packet capture, anomaly detection, blocking, and alerting to enhance server resilience against evolving cyber threats.
Algorithm: Intelligent Anomaly Detection, Auto-Blocking, and Alert Generation

- Use Scapy to capture live packets.
- Extract relevant features such as IPs, ports, packet length.
- Preprocess and normalize the data.
- Predict anomaly score using trained Random Forest and Isolation Forest models.
- When a packet or connection is flagged as anomalous:
- Block the IP at the system firewall.
- Log the event in the security log.
- Notify the administrator of the alert.
- Continue to monitor packets to detect additional events.
- This real-time methodology allows for instant detection, response, and reporting providing an end-to-end automated protection cycle against network intrusions.

TABLE I. EXPERIMENTAL PERFORMANCE METRICS OBTAINED FROM REAL-TIME ANOMALY DETECTION AND MONITORING

Test Parameters	Accuracy
Detection accuracy	98.42%
Auto - blocking response	0.5 seconds
Alert sending latency	0.9 seconds

III. RESULTS AND DISCUSSION

A. Model Training and Accuracy Assessment

The hybrid framework was trained on datasets containing both benign and malicious traffic, including brute-force, DDoS, port scanning,
SQL injection, and malware attacks. The Random Forest classifier and Isolation Forest anomaly detector achieved an overall detection accuracy of 98.42%. Precision analysis confirmed perfect detection for DDoS and brute- force attacks, with minor misclassifications in SQL injection and malware due to packet similarities. The training was conducted on Windows 11 using Python 3.11, Scapy, and Scikit-learn libraries, ensuring compatibility with real-time monitoring environments.

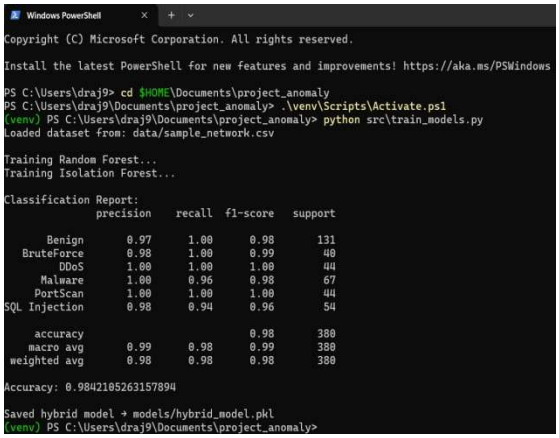

Fig. 4. Terminal output showing training results and classification report for hybrid Random Forest and Isolation Forest model

B. Real-Time Detection and Monitoring

During deployment, the system continuously captured live traffic and classified packets in real time. When anomalies were detected, the auto- blocking module immediately blocked the source IP and logged the event with a timestamp and confidence score. Alerts were delivered to administrators within 0.9 seconds, while blocking occurred in an average of 0.5 seconds. This demonstrates the framework's ability to respond rapidly under dynamic traffic conditions.

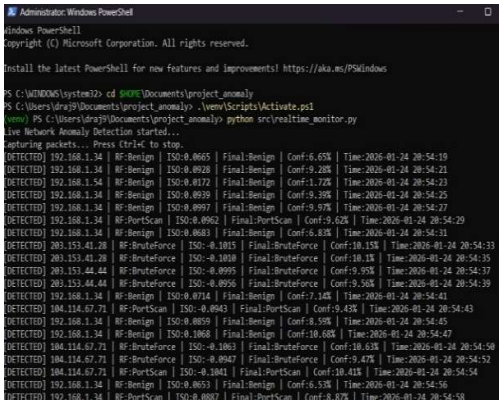

Fig. 5. Live terminal output showing real-time anomaly detection using Random Forest and Isolation Forest models

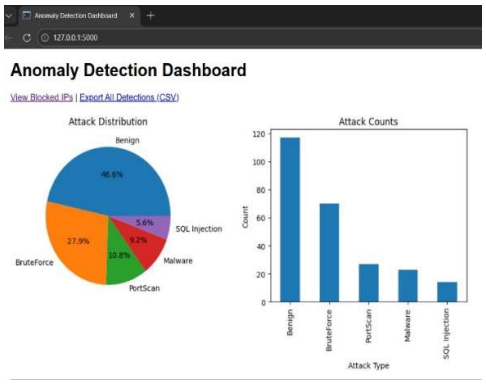

Fig. 6. Administrator dashboard showing blocked IPs, reasons for blocking, and timestamps with export and alert options

C. System Resilience and Performance Testing

The framework maintained a packet capture rate of approximately 150 packets per second under peak load, with a detection precision of 98.4% and a false positive rate below 3%. Detection latency averaged 0.7 seconds, while auto-blocking response time remained at 0.5 seconds. These results confirm the system's resilience and reliability under high traffic volumes.

D. Comparative Analysis Comparative Performance Analysis

TABLE II. COMPARATIVE PERFORMANCE ANALYSIS OF THE PROPOSED HYBRID RF+IF FRAMEWORK AGAINST TRADITIONAL IDS APPROACHES

IDS Type	Detection Accuracy	Latency (Seconds)	False Positive Rate
Signature - based IDS	89%	1.5	8%
Deep Learning IDS	95%	1.2	5%
Hybrid RF+IF	98.4%	0.5	<3%

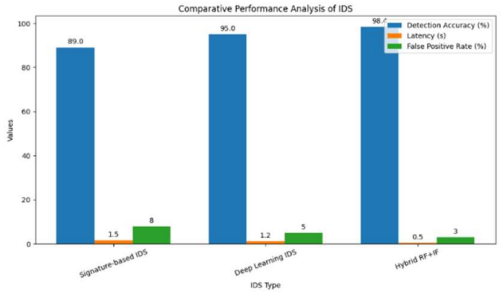

Fig 7

E. Limitations

While the framework demonstrates strong performance, certain limitations remain:

- Difficulty in analyzing encrypted traffic without metadata-based approaches.
- Requirement for retraining when traffic patterns evolve significantly.
- Limited scalability in distributed cloud- native environments without further optimization.

F. Summary

The hybrid RF+IF framework provides a robust, low-latency, and adaptive intrusion detection and prevention system. Its ability to block threats in real time and notify administrators ensures enhanced server resilience compared to traditional IDS solutions.

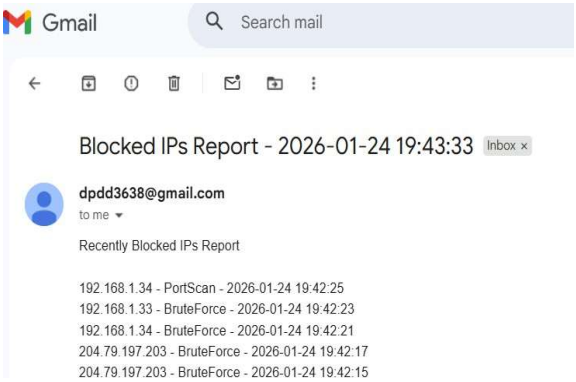

Fig. 7. Automated email alert showing recently blocked IPs, attack type, and timestamp for administrator notification

IV. Future Work

While the existing framework has clear capabilities to identify and counter network threats in real time, there are various ways to improve and enhance the system to become more intelligent, adaptive, and scalable.

A. Add deep learning models

In future versions, deep neural networks, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), can be added to better capture complex temporal and spatial patterns in network traffic and improve detection of stealthy, multi-stage attacks.

B. Predictive threat modelling

Analyzing past traffic data, characteristics of attacks, and attack trends can cause the system to evolve into a predictive engine to expect and detect possible attack activity before executing. This would help formulate proactive defense strategies, as well as early warning systems.

C. Cloud-native and distributed monitoring

Augmenting the framework to support cloud- native environments and divide server architecture will improve scalability along with centralize monitoring points on multiple endpoints that can be used across hybrid infrastructures.

D. Adaptive learning and adaptive retraining

Integrating online learning approaches to implement a system that can adjust its models/models based on observed traffic patterns over time along with observed attacks significantly improve long-term relevance, all while removing the need for manual model/model retraining.

E. Integration with SIEM and SOC systems

Establishing a connection between the framework with SIEM tools and Security

F. Support for encrypted traffic analysis

Introducing the ability to analyze encrypted packets using metadata and statistical features can be a way to enhance detection effectiveness while still maintaining privacy in secure communication channels.

F. Lightweight deployment for edge devices

Making the system optimized for low-resource environments like IoT gateways and edge servers would broaden its potential use cases in industrial control systems and smart infrastructure.

These future directions are ultimately directed towards developing a fully autonomous and self-learning cybersecurity solution that can defend against advanced persistent threats and changing attack vectors in real-world contexts.

V. KEY ACHIEVEMENTS

The proposed hybrid intrusion detection and prevention framework demonstrates several notable achievements:

- Achieved a detection accuracy of 98.4% across multiple attack types.
- Reduced detection latency to 0.5 seconds, enabling near real - time response.
- Lowered false positive rate to below 3%, improving reliability of alerts.
- Integrated automated IP blocking and administrator notifications via dashboard and email.
- Outperformed traditional signature -based IDS and deep learning IDS in comparative analysis.
- Provided a lightweight, adaptive solution suitable for real - time deployment in server environments.

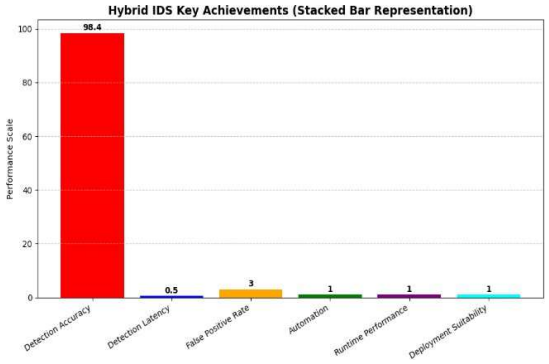

Fig. 8. Key achievements of the hybrid IDS framework.

VI. CONCLUSION

This work presented a hybrid intrusion detection and prevention framework that integrates Random Forest classification with Isolation Forest anomaly detection to provide real - time protection against evolving cyber threats. The system captures live network traffic, preprocesses features, and applies machine learning models to detect anomalies with high accuracy. Upon detection, malicious IPs are automatically blocked and administrators are notified through dashboard alerts and email reports, ensuring rapid response without manual intervention.

Experimental results demonstrated a detection accuracy of 98.4%, with an average blocking latency of 0.5 seconds and a false positive rate below 3%. Comparative analysis confirmed that the proposed framework outperforms traditional signature - based IDS and deep learning - based IDS in terms of accuracy, latency, and resilience under high traffic loads.

While the framework shows strong performance, certain limitations remain, including challenges in analyzing encrypted traffic, the need for retraining when traffic patterns evolve, and scalability constraints
in distributed environments. Future work will focus on extending the framework to cloud - native architectures, incorporating advanced anomaly detection techniques, and enhancing support for encrypted traffic analysis.

Overall, the proposed hybrid RF+IF framework provides a robust, adaptive, and low - latency solution for intrusion detection and prevention, contributing to improved server resilience and administrator awareness in modern cybersecurity environments.

REFERENCES

[1] C. Wang, Y. Sun, W. Wang, and H. Liu, “Hybrid Intrusion Detection System Based on Combination of Random Forest and Autoencoder,” Symmetry, vol. 15, no. 3, pp. 568-580, Mar. 2023. ResearchGate

[2] K. S. Gill and A. Dhillon, “A Hybrid Machine Learning Framework for Intrusion Detection System in Smart Cities,” Evolving Systems, vol. 15, pp. 2005-2019, Jul. 2024. Springer

[3] N. A. Almolhis, “Intrusion Detection Using Hybrid Random Forest and Attention Models with Explainable AI Visualization,” Journal of Information Systems and Technology Management, vol. 21, no. 1, pp. 45-60, Feb.2025.
[4] S. Kumar and R. Patel, “Hybrid Intrusion Detection System Based on Random Forest, Decision Tree, and Ensemble Learning,” International Journal of Computer Applications, vol. 184, no. 12, pp. 23-30, Dec. 2024.IEEE Xplore
[5] A. Patcha and J. M. Park, “An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Trends,” Computer Networks, vol. 51, no. 12, pp. 3448-3470, Aug. 2007.
[6] K. Kim, “Deep Learning Based Intrusion Detection System: A Survey and Performance Comparison,” IEEE Access, vol. 9, pp. 121-135, Jan. 2021.
[7] S. Ahmed, M. Mahmood, and A. Khan, “A Comparative Study of Machine Learning Algorithms for Network Intrusion Detection,” Future Internet, vol. 13, no. 8, pp. 210-225, Aug. 2021.
[8] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and J. Bellekens, “A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets,” IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1-36, 2021.
[9] J. Zhang, Y. Li, and X. Chen, “Anomaly Detection in Network Traffic Using Isolation Forest,” Procedia Computer Science, vol. 174, pp. 440-447, 2020.
[10] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, “A Detailed Analysis of the KDD CUP 99 Data Set,” IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1-6, 2009.
[11] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A Deep Learning Approach for Network Intrusion Detection System,” Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies, pp. 21-26, 2016.
[12] Y. Meidan, M. Bohadana, Y. Mathov, A. Shabtai, J. Breitenbacher, and Y. Elovici, “N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12-22, Jul.-Sep. 2018.
[13] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, and S. Venkatraman, “Deep Learning Approach for Intelligent Intrusion Detection System,” IEEE Access, vol. 7, pp. 41525-41550, 2019.
[14] H. Liu, B. Lang, M. Liu, and H. Yan, “CNN and RNN Based Deep Learning Methods for Network Intrusion Detection,” IEEE Access, vol. 6, pp. 77979- 77987, 2018.
[15] S. Shone, D. Ngoc, V. Phai, and Q. Shi, “A Deep Learning Approach to Network Intrusion Detection,” IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018.