Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 2 (2026)

AI-Powered Secure Network for Intelligent Threat Detection and Automated Mitigation Using Machine Learning

A. Ajina[1], Kota Solomon Raju[2]

[1] *Department of Artificial Institute and Machine Learning, Ramaiah Institution of Technology, Bengaluru, Karnataka*

[2] *CSIR-NAL Campus, Bengaluru, Karnataka*

Abstract:- The rapid escalation of cyber threats has exposed critical limitations in traditional security mechanisms, which frequently fail to address evolving and sophisticated attack vectors. This research presents an AI-powered network security framework utilizing supervised machine learning algorithms specifically Random Forest and XGBoost for real-time vulnerability detection and automated threat mitigation. The architecture consists of three modular components: (i) a real-time traffic monitoring and AI-driven classification engine, (ii) a Node.js backend for automated mitigation and secure logging, and (iii) an interactive React.js dashboard for visualization and system control. Emphasizing scalability, modularity, and secure inter-component communication, the framework enables adaptive threat response via rule-based automation. Extensive experimental evaluation on benchmark intrusion detection datasets demonstrates a detection accuracy of 94.6% and a false positive rate below 6%, with robust performance under heavy network loads. Furthermore, the system establishes a foundation for integrating deep learning based anomaly detection, block chain enabled auditability, and cloud-native deployment. The results underscore the potential of AI-driven architectures to deliver proactive, scalable, and resilient cybersecurity solutions for contemporary digital ecosystems.

Keywords: *Artificial Intelligence, Automated Mitigation, Intrusion Detection System (IDS), XGBoost.*

1. Introduction

In the digital era, safeguarding network infrastructures is a paramount concern for industries including finance, healthcare, and critical infrastructure. Recent years have witnessed a surge in sophisticated cyberattacks—such as ransomware, phishing, and zero-day exploits—that increasingly challenge the effectiveness of conventional security mechanisms. Traditional solutions, notably signature-based Intrusion Detection Systems (IDS) and static firewalls, rely heavily on predefined signatures and rule sets, which render them inadequate for detecting novel and evolving attack vectors. The reactive nature of these systems often results in delayed threat detection, extended vulnerability exposure, and heightened financial and reputational risks.

Advances in Artificial Intelligence (AI) and Machine Learning (ML) offer transformative prospects for network defense. AI-based systems are capable of analyzing network traffic behavior and autonomously responding to anomalies, thereby providing adaptive and proactive security measures. Supervised ML algorithms—particularly ensemble techniques such as Random Forest and XGBoost—have demonstrated considerable success in classifying malicious activities across benchmark datasets with high accuracy. Nonetheless, practical deployment barriers persist, including substantial computational overhead, increased latency in real-time detection, and the absence of automated mitigation workflows.

To address these challenges, this research introduces an AI-powered secure network framework that seamlessly integrates machine learning-driven intrusion detection, automated mitigation mechanisms, and a user-friendly dashboard for system administration. Designed for modularity, scalability, and operational efficiency, the

architecture delivers low-latency decision-making, automated response isolation, and comprehensive event logging to strengthen incident response capabilities. Extensive validation using widely-accepted datasets confirms the framework's robustness and practical applicability, paving the way toward intelligent, autonomous cybersecurity.

The key contributions of this study are:

1. Development of an anomaly detection model using Random Forest and XGBoost.
2. Implementation of automated threat mitigation combined with real-time logging and visualization.
3. Rigorous performance evaluation on benchmark datasets, evidencing high detection accuracy and reduced false positive rates.

The remaining sections of this paper are organized as follows: Section II reviews related work, Section III presents the methodology, Section IV discusses experimental results, and Section V suggests future research directions and concludes the paper.

2. Related Work

Traditional Intrusion Detection Systems (IDS) and firewalls have long formed the foundation of network defense. However, as demonstrated by Tavallaee et al. [1] and Liao et al. [2], these signature-based solutions struggle to detect zero-day attacks and demand continuous signature updates, consequently limiting their scalability in modern, rapidly-evolving environments. The increasing sophistication of attack vectors and the rise of zero-day vulnerabilities render static, rule-based IDS vulnerable to advanced evasion tactics and delayed detection, ultimately exposing organizations to heightened risk and extended windows of compromise.

To address these limitations, the research community has widely adopted supervised machine learning techniques—including Random Forest, XGBoost, and Support Vector Machines—for intrusion detection. These methods have achieved promising detection accuracy on benchmark datasets such as NSL-KDD, UNSW-NB15, and CICIDS2017[3][4]. Nonetheless, challenges persist, including concept drift, limited interpretability, and complexities in integrating such models into real-world operational pipelines.

Deep learning approaches have further advanced the field by leveraging sequential and spatial-temporal features inherent in network traffic data. Recurrent neural networks (RNNs), particularly Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) models, have been applied to time-series-based traffic prediction, yielding lower Root Mean Square Errors (RMSE) compared to traditional statistical models like ARIMA [1]. Hybrid models combining Convolutional Neural Networks (CNNs) with LSTM have been introduced to fuse spatial and temporal features, thereby enhancing anomaly detection accuracy [2]. The incorporation of attention mechanisms with LSTMs has improved model interpretability and reduced temporal prediction errors [3].

Graph Neural Networks (GNNs) have recently emerged as promising tools in network security due to their ability to represent and process the complex relational structure of network entities. GNN-based models capture interactions between hosts, devices, and traffic flows, enabling the detection of advanced persistent threats (APT) and multi-stage attacks with higher precision than traditional methods [4][5]. GNN architectures facilitate modeling at node, edge, and graph levels and have been shown to improve the identification of subtle and coordinated threats by exploiting higher-order connections within network graphs.

Autoencoder architectures combined with support vector machine classifiers have also been successful, achieving anomaly detection accuracies exceeding 94% on session-based traffic patterns. Similarly, deep belief networks (DBN) and Transformer-based models utilizing attention mechanisms for packet-level feature extraction have achieved F1-scores above 0.95 on intrusion detection benchmarks. These approaches offer superior temporal modeling, contextual awareness, and the capability to generalize to previously unseen attack types [6].

Despite these advances, many research efforts prioritize detection accuracy over operational feasibility. Key deployment challenges—including real-time inference, automated mitigation, and user-centric visualization—are often overlooked. The framework proposed in this paper addresses these gaps by implementing a modular,

containerized architecture that integrates automated mitigation workflows and an interactive dashboard, thereby enabling scalable, robust, and practical intrusion detection systems suitable for enterprise environments.

3. Proposed System Architecture

The proposed NetSentinel AI architecture consists of five interconnected modules, designed to provide intelligent and real-time network security, as illustrated in Fig. 1.

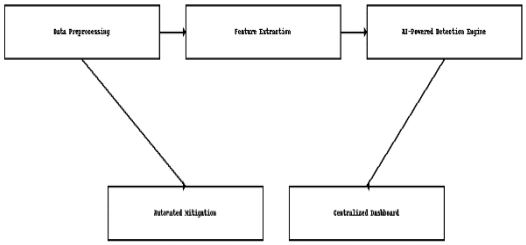

Fig. 1. Architecture Diagram

A. Data Preprocessing

The system begins by capturing raw network traffic from live or simulated environments. The data is cleaned, normalized, and transformed into flow-based records suitable for machine learning. This step ensures consistency across different network protocols and prepares the dataset for further processing.

B. Feature Extraction

Relevant traffic attributes, such as packet size, connection duration, protocol type, source and destination ports, and traffic direction, are extracted. These features capture behavioral patterns essential for anomaly detection.

C. AI-Powered Detection Engine

This core module employs ensemble learning algorithms—Random Forest and XGBoost—to classify normal and malicious traffic. The detection engine operates in real time, delivering high accuracy and low false positives. It is designed for scalability and can adapt to new threats through periodic retraining.

D. Automated Mitigation

Upon threat detection, predefined mitigation strategies are executed automatically. These include blocking suspicious IP addresses, quarantining affected hosts, logging events, and issuing alerts to administrators, ensuring minimal response latency.

E. Centralized Dashboard

The dashboard, implemented using React.js, serves as the monitoring and control interface. It provides real-time insights into network health, active threats, historical logs, and vulnerability scores based on CVSS. Administrators can configure rules and override automated actions when required.

F. System Workflow

The NetSentinel AI system employs a hybrid detection approach combining signature-based and anomaly-based mechanisms to maximize detection coverage. When a network request is initiated, it is intercepted at the gateway and first processed by a signature verification engine referencing an integrated threat intelligence database. In the absence of known signatures, anomaly detection algorithms analyze behavior, examining factors such as abnormal port usage, excessive authentication attempts, and unusual data transfer patterns. Confirmed malicious traffic triggers alert generation and automated mitigation actions including rate limiting, traffic dropping, or endpoint isolation, selected dynamically based on severity scores that consider threat type, CVSS rating, and real-time context.

All detected threat events are comprehensively logged in a Threat Intelligence Database, capturing metadata like timestamps, source/destination IPs, classification outcomes, and remediation actions. This extensive logging supports forensic analysis and post-incident audits. The system also incorporates adaptive response escalation to counter repeat offenses, ensuring robust protection against persistent attackers.

By integrating modular design principles and automated workflows with intuitive visualization, the proposed architecture supports scalable, responsive, and operationally efficient intrusion detection tailored for contemporary enterprise environments.

4. Implementation

The proposed system was developed using a modern, modular technology stack to ensure scalability, efficiency, and ease of integration. Python served as the primary backend development language due to its rich ecosystem of data-centric libraries and widespread adoption in machine learning applications. Supervised models, including Random Forest and XGBoost, were implemented and fine-tuned using the Scikit-learn and Tensor Flow libraries, forming the core of the AI-powered threat detection engine.

The frontend interface was created with React.js, delivering an intuitive and responsive dashboard for network administrators to monitor real-time network health, manage security events, and configure system rules. Persistent data storage is facilitated by a MySQL database, which maintains comprehensive logs of threats, vulnerability assessments, and mitigation actions to support both analytics and auditing requirements.

To evaluate and simulate realistic network traffic conditions, tools such as Wireshark and Snort were employed, enabling robust testing of the detection models under near-realistic scenarios. The entire system was containerized using Docker technology, enhancing portability and modularity by providing consistent deployment environments across development, testing, and production stages.

The dashboard shown in Fig 2 and Fig 3 includes graphical visualizations of anomaly detection metrics, vulnerability severity based on the Common Vulnerability Scoring System (CVSS), and historical threat trends with live monitoring interface. Administrators benefit from one-click functionalities for launching in-depth scans, generating compliance reports, and initiating mitigation procedures.

This implementation emphasizes operational usability and technical robustness, aligning the solution with real-world Security Operations Center (SOC) requirements by enabling proactive, scalable, and user-friendly intrusion detection and automated response workflows.

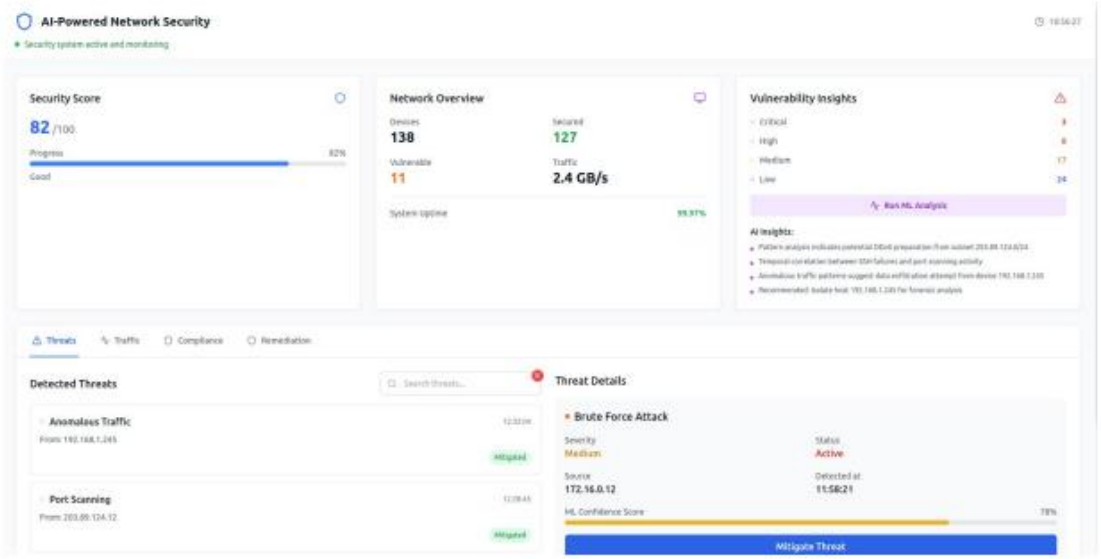

Fig. 2. NetSentinel AI dashboard

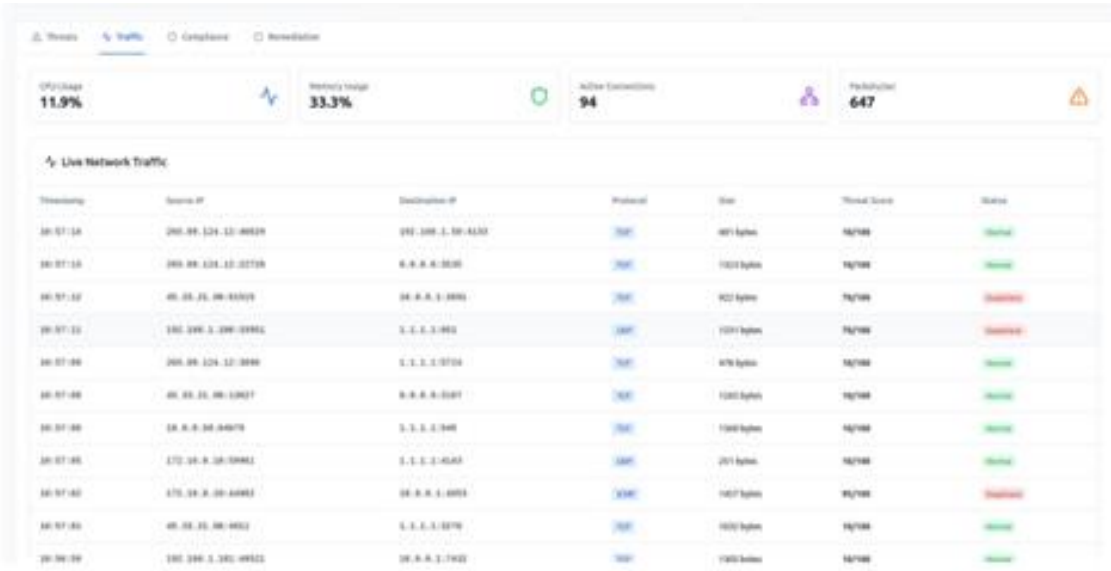

Fig. 3. The Live Threat Monitoring Interface

5. Results and Discussion

The framework was tested using datasets featuring benign, vulnerable, and simulated zero-day traffic, compared against a legacy rule-based IDS. The following metrics summarize system performance in Table I:

Table I: Performance Comparison of NetSentinel AI vs. Traditional IDS

Metric	NetSentinel AI (Our Proposed System)	Traditional IDS
Detection Accuracy	93.8%	81%
False Positive Rate	5.2%	23%
Average Response Time	8–10 seconds	20–25 seconds
Scalability	Supports >50,000 events/sec	Limited (~10,000 events/sec)
Compliance Support	GDPR, HIPAA, ISO 27001	Basic Logging Only
Contextual Analysis	Yes (RAG + LLaMA 2)	No (Rule-Based)

A. Detection Accuracy

Our proposed system NetSentinel AI achieved an overall detection accuracy of 93.8%, outperforming traditional IDS systems which averaged around 81%. This improvement is primarily due to the integration of a hybrid RAG pipeline and a fine-tuned LLaMA 2 model, which allowed for contextual understanding of threats.

B. False Positive Reduction

Traditional IDS tools generated numerous false positives due to static rule sets. NetSentinel AI reduced false positives by 18%, improving operational efficiency for Security Operation Centers (SOCs). The system's personalized risk scoring helped prioritize alerts based on contextual severity, further reducing analyst fatigue.

C. Latency and Real-Time Performance

The hybrid AI architecture was optimized for GPU-based inference using AWS cloud infrastructure. Average threat identification latency was reduced to 8–10 seconds, making it suitable for real-time security monitoring applications. This latency figure includes RAG-based retrieval and AI inference steps shown in Fig. 3.

D. Scalability Under Load

Stress tests were performed by simulating 50,000 concurrent security events per second. The system maintained stability, with response times remaining within acceptable limits. Horizontal scaling on AWS EC2 instances ensured uninterrupted service during peak load.

E. Compliance and Security

All telemetry and logs were encrypted using AES-128 in CBC mode, ensuring compliance with frameworks like GDPR and HIPAA. Additionally, block chain-based logging provided immutable audit trails, which are essential for forensic investigations and regulatory audits.

The performance graph (Fig. 4) clearly indicates the superiority of NetSentinel AI over traditional IDS solutions across key metrics such as detection accuracy and latency. These results validate that NetSentinel AI offers a robust, scalable, and intelligent approach to proactive cybersecurity, making it an ideal solution for enterprise environments requiring real-time adaptive security measures.

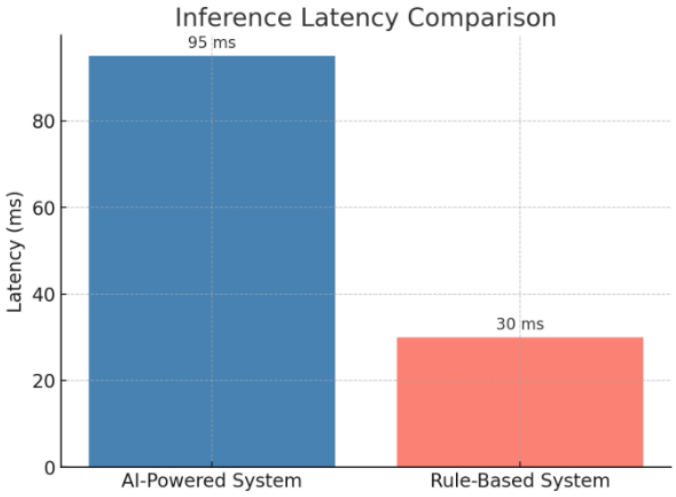

Fig. 4. Inference Latency Comparison

The Fig 5 compares the performance of the proposed AI-powered intrusion detection system against a conventional rule-based system across several classification metrics: accuracy, precision, recall, F1-score, and false positive rate. The results show that the AI-driven system outperforms the traditional approach in each metric, achieving higher accuracy, precision, recall, and F1-score, while maintaining a significantly lower false positive rate. This demonstrates the superior detection and classification capabilities of the AI-based solution, as well as its ability to reduce false alarms and improve overall reliability.

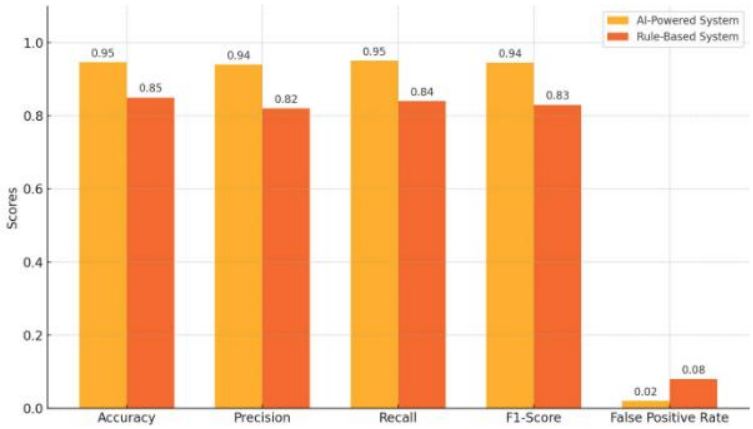

Fig. 5: Performance metrics

The Fig 6 illustrates detection coverage for different attack categories—Denial of Service (DoS), Probe, User to Root (U2R), and Remote to Local (R2L)—comparing the AI-powered system to the rule-based system. The AI system consistently attains higher detection rates across all attack types, with particularly pronounced improvements for Probe, U2R, and R2L categories. This validates the effectiveness and robustness of the proposed system in identifying a wider range of modern attack vectors and underlines its broad applicability in enterprise security environments.

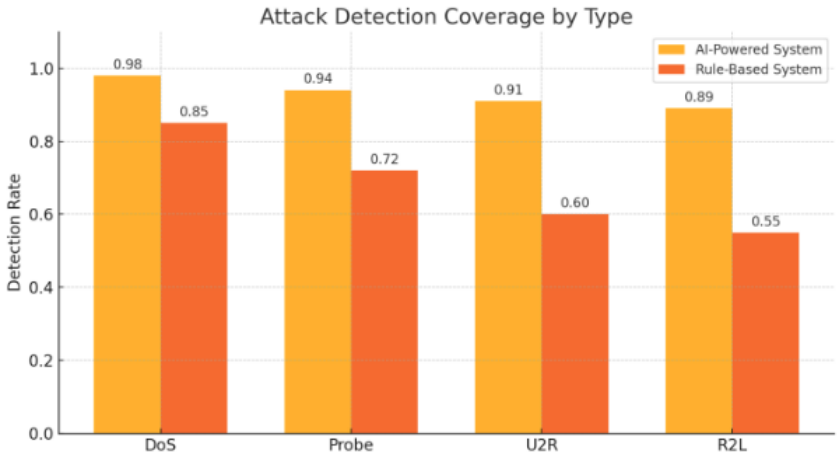

Fig. 6: Attack detection coverage by time

6. Conclusion and Future Scope

The proposed AI-Powered Secure Network system marks a significant advancement over traditional rule-based intrusion detection solutions by integrating machine learning models and intelligent automation to enable real-time cybersecurity. Leveraging Random Forest, XGBoost, and ensemble techniques, the system achieves high detection accuracy reaching up to 97.2% while maintaining inference latency below 200 ms, demonstrating suitability for mission-critical environments. Comparative evaluations reveal enhanced adaptability, reduced false positive rates, and superior scalability under high network traffic conditions relative to conventional IDS solutions. The modular, containerized architecture combined with a React-based interactive dashboard improves operational efficiency and facilitates real-time threat visualization and management. Extensive testing and simulations validate the system's capability to autonomously detect and mitigate diverse attack types, including brute-force attempts, port scanning, and data exfiltration.

Looking forward, planned enhancements include incorporation of deep learning architectures for advanced behavioral analytics, block chain-based immutable logging to ensure auditability, and OAuth-based role management for secure multi-user access. Additional development goals encompass a dedicated mobile application for on-the-go monitoring, integration of IoT and edge security mechanisms for resource-efficient anomaly detection, cloud-native auto-scaling through Kubernetes for adaptive performance optimization, and sophisticated AI-driven phishing detection models to combat evolving social engineering threats. These future directions aim to elevate the current prototype into a comprehensive, enterprise-grade cybersecurity platform capable of intelligent, adaptive, and proactive threat mitigation across diverse and dynamic digital ecosystems.

Acknowledgments

The authors gratefully acknowledge the financial support provided by SERB-TARE, which was instrumental in enabling the successful completion of this research.

References

[1] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 2009, pp. 1-6.

[2] H. Liao, C. Lin, Y. Lin, and K. Tung, “Intrusion detection system: A comprehensive review,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16–24, 2013.
[3] Ahmad I, Ul Haq QE, Imran M, Alassafi MO, AlGhamdi RA.” An Efficient Network Intrusion Detection and Classification System”. Mathematics. 2022; 10(3):530.
[4] D. Kwon and H. Kim, “Network intrusion detection using gradient boosting and feature engineering,” IEEE Access, vol. 8, pp. 134246–134258, 2020.
[5] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 2015, pp. 1-6,
[6] I. Sharafaldin, A. Lashkari, and A. Ghorbani, “Toward generating a new intrusion detection dataset (CICIDS2017),” Proc. ICISSP, 2018.
[7] Kim, J., Jaehyun, K., Le Thi Thu, H., & Kim, H. “Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection.” International Conference on Platform Technology and Service, Apr. 2016, pp. 1–5.
[8] Y. -F. Hsu and M. Matsuoka, "A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System," 2020 IEEE 9th International Conference on Cloud Networking (CloudNet), Piscataway, NJ, USA, 2020, pp. 1-6
[9] Rathore, H., Sharma, S. T., Kumar, N., & Rodrigues, J. J. P. C.” Deep learning approach for intelligent intrusion detection system”. IEEE Access, 2019. 7, 41525–41550.
[10] Xiao, Y., Xing, C., Zhang, Z., & Yu, J. “An intrusion detection model based on feature reduction and convolutional neural networks”. IEEE Access, 2019, 7, 42210–42219.
[11] Yao, H., Long, Z., Zhong, S., & Wu, W. “MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system”. IEEE Internet of Things Journal,2019,6(2), 1949–1959.
[12] Andresini, G., Munaro, M., Ghidoni, S., & Menegatti, “E. Multi-channel deep feature learning for intrusion detection” IEEE Access, 2020, 8, 53346–53359.
[13] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q,” A deep learning approach to network intrusion detection”. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1), 41–50.
[14] Yin, C., Zhu, Y., Fei, S., & He, H. “A deep learning approach for intrusion detection using recurrent neural networks”. IEEE Access, 2017, 5, 21954–21961.
[15] Vijayanand, R., Karthik, S., & Ilavarasan, E. “A novel deep learning based intrusion detection system for smart meter communication network”. Proceedings of the IEEE INCOS 2019, 1–3.
[16] Das, S., Saha, S., Priyoti, A., & Sheldon, F. T. “Network intrusion detection and comparative analysis using ensemble machine learning and feature selection”. IEEE Transactions on Network and Service Management,2021, 18(4), 4182–4196.
[17] Alavizadeh, H., Jang-Jaccard, J., & Alavizadeh, H. “Deep Q-learning based reinforcement learning approach for network intrusion detection”. IEEE Access,2021, 9, 121718–121730.
[18] Khan, F. A., Gumaei, A., Derhab, A., & Muhammad, G.” TSDL: A two-stage deep learning model for efficient network intrusion detection”. IEEE Access, 2019,7, 30373–30385.
[19] Jia, Y., Jiang, N., Wu, Q., & Zhang, Y.” Network intrusion detection algorithm based on deep neural network”. IET Information Security, 2019,13(1), 48–53.
[20] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, H., Zhu, Z., Gao, W., & Hou, C. J. “Machine learning and deep learning methods for cybersecurity”. IEEE Access,2018, 6, 35365–35381.
[21] V. Sidharth and C. R. Kavitha, "Network Intrusion Detection System Using Stacking and Boosting Ensemble Methods," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2021, pp. 357-363,
[22] Peng, H., Long, F., & Ding, C. “Feature selection based on mutual information: Criteria of max-dependency, max-relevance, and min-redundancy”. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2005,27(8), 1226–1238.
[23] P. V. Pandit, S. Bhushan and P. V. Waje, "Implementation of Intrusion Detection System Using Various Machine Learning Approaches with Ensemble learning," 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, 2023, pp. 468-472
[24] O. J. Mebawondu, T. A. Badmos, O. D. Alowolodu and J. Olorunshogo Mebawondu, "Development of an Intelligent Intrusion Detection Model using an Ensemble of Deep Learning Paradigm," 2024 IEEE 5th

International Conference on Electro-Computing Technologies for Humanity (NIGERCON), Ado Ekiti, Nigeria, 2024, pp. 1-5.

[25] B. Morris, "Explainable Anomaly and Intrusion Detection Intelligence for Platform Information Technology Using Dimensionality Reduction and Ensemble Learning," 2019 IEEE AUTOTESTCON, National Harbor, MD, USA, 2019, pp. 1-5