iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77527

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

Hybrid Anomaly and Signature-Based Approach for Network Attack Detection

V T Ram Pavan Kumar[1], Paila Yerri Naidu[2], Nhs Pavan Kumar[3], S Gopala Krishna[4], D Yaswanth Kumar[5], G Nikesh[6], Akash Jannigorla[7], Chopparapu Venugopal[8]
[1]*Associate Professor, Department of Computer Science*
[2, 3, 4, 5, 6, 7, 8]*II MCA*
[1,2,3,4,5,6,7,8]*Kakaraparti Bhavanarayana College, Vijayawada, Andhra Pradesh*

Abstract: ***With the rapid expansion of interconnected systems and digital infrastructures, network environments face increasingly complex and dynamic cyber threats. Traditional signature-based detection systems are effective against known attacks but fail to detect zero-day and evolving threats. Conversely, anomaly-based detection systems can identify unknown behaviours but often suffer from high false positive rates. This research proposes a hybrid intrusion detection framework that integrates signature-based and anomaly-based techniques to enhance detection accuracy and reduce false alarms. The model combines pattern matching for known threats with machine learning-driven behavioural analysis for unknown attack detection. Experimental analysis demonstrates that the hybrid approach significantly improves detection rates, lowers false positives, and provides adaptive Défense capabilities suitable for modern enterprise and cloud network environments.***
Keywords: Network Security, Intrusion Detection System, Hybrid Detection, Signature-Based Detection, Anomaly Detection, Machine Learning, Cyber Attacks, Zero-Day Attacks, Network Monitoring, Threat Detection.

I. INTRODUCTION

Network security has become a critical concern due to the increasing frequency and sophistication of cyber attacks. Organizations rely heavily on digital networks to store, process, and transmit sensitive information. Attackers exploit vulnerabilities through malware, Distributed Denial-of-Service (DDoS) attacks, phishing, ransomware, and advanced persistent threats (APTs).

Traditional Intrusion Detection Systems (IDS) typically employ either signature-based or anomaly-based detection mechanisms. Signature-based systems are efficient in identifying previously known threats using predefined patterns but cannot detect new or modified attacks. Anomaly-based systems monitor deviations from established behavioral norms and can detect unknown threats but often generate high false positives.

To overcome these limitations, this research proposes a hybrid detection framework that combines both approaches to achieve improved accuracy, adaptability, and efficiency in network attack detection.

II. LITERATURE SURVEY

The rapid evolution of cyber threats has driven significant research toward improving intrusion detection systems (IDS), particularly through hybrid approaches that combine signature-based and anomaly-based techniques. Traditional signature-based IDS are effective in detecting known attack patterns but fail to identify novel or zero-day threats. In contrast, anomaly-based systems can detect unknown behaviors but often suffer from high false positive rates. To overcome these limitations, researchers have proposed hybrid frameworks that integrate both mechanisms to enhance detection accuracy and reduce false alarms [1], [2]. Recent studies emphasize the integration of deep learning models within hybrid IDS architectures. Huang *et al.* proposed a hybrid deep learning model combined with federated learning for intrusion detection in distributed environments. Their approach integrates convolutional neural networks and attention mechanisms to improve feature extraction and classification performance while maintaining data privacy. Experimental results demonstrated improved detection accuracy and reduced communication overhead in distributed network settings [1]. Similarly, Sadhwani *et al.* introduced a hybrid CNN–BiLSTM architecture for IoT intrusion detection, effectively capturing both spatial and temporal traffic features. The proposed model achieved high accuracy and robustness across multiple benchmark datasets, highlighting the importance of combining multiple deep learning techniques within hybrid IDS frameworks [2]. Feature selection and optimization techniques also play a crucial role in hybrid IDS performance. Ayad *et al.* proposed a hybrid feature selection method combining filter and wrapper approaches to enhance anomaly detection in IoT networks.

Their method improved classification accuracy while reducing computational complexity, making it suitable for real-time detection systems [3]. Furthermore, Aldawood *et al.* developed a hybrid anomaly–rule–pattern detection framework that integrates rule-based signature detection with unsupervised anomaly detection techniques. Their streaming-based architecture effectively detected persistent and stealthy attacks, demonstrating improved resilience against evolving cyber threats [4]. In addition, ensemble-based hybrid approaches have gained attention for improving robustness and generalization. Alharbi and Khan proposed an ensemble hybrid IDS model combining multiple machine learning classifiers to detect diverse attack categories. Their framework demonstrated superior performance compared to standalone classifiers by leveraging complementary strengths of different algorithms [5]. Baidar *et al.* further extended hybrid IDS research by integrating deep learning with federated learning in IoT and 5G networks. Their distributed hybrid architecture achieved high detection rates while preserving user data privacy, making it suitable for next-generation network infrastructures [6]. Recent advancements in network security and intelligent systems have significantly contributed to strengthening cyber defense mechanisms in modern infrastructures. Manikandan and Srilakshmi proposed a deep learning-based vulnerability detection and mitigation framework for virtualization data centers, focusing on identifying security weaknesses within virtual machine environments. Their approach leverages deep neural networks to detect abnormal behavior patterns and proactively mitigate potential risks, thereby improving resilience and resource utilization in cloud-based infrastructures [7].

In another study, Manikandan and Srilakshmi introduced an HMM-assisted proactive vulnerability mitigation technique using controlled virtual machine placement strategies. By integrating Hidden Markov Models with dynamic VM allocation, the framework predicts potential security threats and minimizes attack surfaces within virtualized environments. The research demonstrates improved threat prediction accuracy and optimized resource management in data centers [8]. Expanding toward community network analysis, Manikandan *et al.* investigated the linear degree of community network patterns to reduce misclassification issues in machine learning-based classification systems. Their study highlights the importance of structural network feature analysis in improving classification robustness and eliminating false interpretations in large-scale network data processing [9]. Badonia *et al.* examined the implications and challenges in modernizing healthcare systems using 5G technologies. Their research discusses security vulnerabilities introduced by high-speed connectivity and emphasizes the need for secure communication protocols and adaptive cybersecurity mechanisms in next-generation healthcare infrastructures [10]. Shaik *et al.* explored physical layer security mechanisms for wireless sensor networks (WSNs), addressing challenges such as eavesdropping and energy constraints. Their work proposes optimized physical layer techniques to enhance secure data transmission while maintaining energy efficiency, which is critical for resource-constrained network environments [11]. Pande *et al.* proposed a dynamic security bounds framework to improve both efficiency and security in IoT networks. The framework enhances encryption boundaries and adaptive access control mechanisms to protect IoT devices from emerging cyber threats, demonstrating improved performance under dynamic network conditions [12]. Reddy *et al.* conducted an empirical assessment of deep learning models for profit prediction, highlighting the effectiveness of neural network architectures in predictive analytics. Although primarily focused on financial forecasting, their study demonstrates the adaptability of deep learning techniques in analyzing complex datasets, which can also be extended to cyber threat intelligence systems [13]. Gupta *et al.* developed an optimized swarm intelligence approach combined with fuzzy clustering for intrusive behavior detection in IoT and network systems. Their method enhances anomaly detection accuracy by integrating bio-inspired optimization with clustering mechanisms, thereby improving intrusion detection efficiency in distributed environments [14]. Sahith *et al.* applied ultrasonic bioacoustics with deep learning for early plant disease prediction. While primarily agricultural in focus, their study demonstrates the power of deep learning-based pattern recognition and signal analysis, which can be similarly applied to anomaly detection in cybersecurity systems [15]. Vikruthi *et al.* designed and developed an IoT-based smart women security gadget that integrates real-time tracking, alert mechanisms, and communication technologies. The study highlights practical applications of IoT security and embedded systems in ensuring user safety, emphasizing secure data transmission and device authentication [16]. In another work, Vikruthi *et al.* proposed a deep learning-based system for detecting emergency vehicles and assigning traffic-free paths. Their research illustrates the application of real-time image processing and neural network models for intelligent decision-making in smart transportation systems, reinforcing the role of AI-driven frameworks in secure and adaptive networked systems [17]. This work proposes a Java-based deep learning framework for detecting known and unknown cyberattacks in IIoT systems, combining high accuracy with explainable AI for transparency. Experiments on benchmark datasets show the framework delivers real-time, reliable, and scalable protection for large-scale industrial applications [18]. This paper presents a low-cost upper-limb rehabilitation device equipped with sensors and in-built technology for accurate movement and muscle force evaluation.

The system integrates multiple mechanical structures, driver circuits, a database, and an interactive interface, with key components produced using 3D printing and control implemented via DSPIC30F4011 and stepper motors. The design allows low step angles, torque and pressure monitoring, assisted or resisted limb motion, and real-time data storage and analysis through a Windows-based application, with all parameters verified through testing [19]. This study proposes a home-based upper-limb rehabilitation robot with a current-controlled buck converter for precise movement and muscle force measurement, supporting post-COVID-19 recovery. It features IoT-enabled real-time monitoring of vital signs, cloud data storage, and remote doctor access via a Windows application for continuous patient supervision [20]. Collectively, these studies contribute to advancements in deep learning, IoT security, virtualization security, wireless network protection, and intelligent system design. The integration of machine learning, optimization algorithms, and secure communication frameworks across these works highlights the growing emphasis on adaptive and intelligent cybersecurity mechanisms in modern network environments.

III. SYSTEM ARCHITECTURE

The proposed system architecture figure 1 integrates both signature-based and anomaly-based detection mechanisms to enhance network attack identification accuracy. It processes network traffic through data collection, preprocessing, dual detection engines, and a decision fusion module to generate reliable alerts and automated response actions.

A. Data Collection Module

The Data Collection Module is responsible for capturing real-time network traffic from routers, switches, firewalls, and servers. It collects packet-level and flow-level information such as source/destination IP addresses, ports, protocols, packet size, and timestamps. This module ensures continuous monitoring of incoming and outgoing network traffic without affecting system performance. The collected raw data is forwarded to the preprocessing stage for further analysis.

B. Pre-processing Module

The Preprocessing Module prepares raw network data for analysis. It performs tasks such as data cleaning, removal of redundant packets, handling missing values, and normalization of numerical features. Feature extraction techniques are applied to derive relevant attributes (e.g., traffic rate, session duration, failed login attempts). Dimensionality reduction methods may also be used to improve efficiency. This module ensures structured and optimized input for detection engines.

C. Signature-Based Detection Engine

This engine detects known attacks by comparing incoming traffic patterns with a predefined database of attack signatures. These signatures include patterns of known malware, intrusion attempts, and exploit behaviors. If a match is found, the system immediately flags the traffic as malicious. This module provides high accuracy for previously identified threats but requires regular updates to maintain effectiveness against newly discovered attacks.

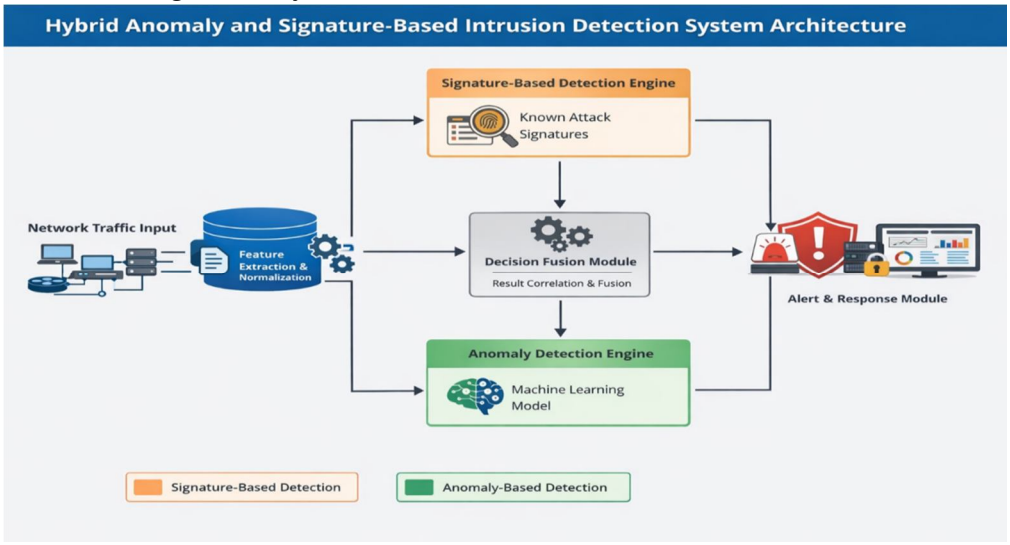


Figure 1: Archtiecture

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue II Feb 2026- Available at www.ijraset.com

D. Anomaly Detection Engine

The Anomaly Detection Engine identifies unknown or zero-day attacks by analyzing deviations from normal network behavior. It uses machine learning models such as Random Forest, Support Vector Machines (SVM), or Neural Networks to establish a baseline of legitimate activity. When unusual patterns or abnormal traffic behavior are detected, the system classifies them as potential threats. This module enhances adaptability but may generate false positives if not properly trained.

E. Decision Fusion Module

The Decision Fusion Module combines outputs from both the signature-based and anomaly detection engines. It applies rule-based logic or weighted scoring mechanisms to correlate detection results. If both engines identify malicious activity, the confidence level increases. In cases of conflict, the module evaluates predefined thresholds to determine the final classification. This integration reduces false positives and improves overall detection accuracy.

F. Alert and Response Module

The Alert and Response Module generate real-time alerts for detected threats and initiates automated mitigation actions. Alerts may be sent to system administrators via dashboards, email notifications, or security information systems. Automated responses include blocking suspicious IP addresses, isolating compromised systems, updating firewall rules, or terminating malicious sessions. This module ensures rapid containment and minimizes potential damage to the network.

IV. METHODOLOGY

A. Dataset

The system is trained and evaluated using benchmark intrusion detection datasets such as NSL-KDD or CICIDS datasets, which contain labeled normal and attack traffic samples.

B. Feature Extraction

Key network features include:

1) Source and destination IP
2) Protocol type
3) Packet size
4) Flow duration
5) Number of failed login attempts
6) Traffic rate

Feature selection techniques such as Principal Component Analysis (PCA) are used to reduce dimensionality and improve model efficiency.

C. Machine Learning Model

The anomaly detection module employs supervised learning algorithms such as:

1) Random Forest
2) Support Vector Machine (SVM)
3) Artificial Neural Networks (ANN)

Model training involves splitting the dataset into training and testing sets, followed by performance evaluation using standard metrics.

V. RESULTS

The table presents a comparative performance analysis of three network attack detection approaches: Signature-Based, Anomaly-Based, and Hybrid Model, evaluated using Accuracy, False Positive Rate, and Detection Rate. The Accuracy metric shows that the Hybrid Model achieves the highest accuracy of 97%, compared to 93% for the Anomaly-Based approach and 91% for the Signature-Based method. This indicates that combining both detection techniques significantly improves overall classification correctness. In terms of False Positive Rate, the Hybrid Model records the lowest rate at 3%, while Signature-Based and Anomaly-Based approaches show 6% and 8% respectively. A lower false positive rate means fewer legitimate network activities are incorrectly classified as attacks, which improves system reliability and reduces unnecessary alerts.

For Detection Rate, which measures the system's ability to correctly identify actual attacks, the Hybrid Model again outperforms the others with 98%. The Anomaly-Based model detects 94% of attacks, while the Signature-Based system detects 89%. This demonstrates that the hybrid approach effectively identifies both known and unknown threats. Overall, the table clearly indicates that integrating signature-based and anomaly-based techniques enhances detection performance, increases accuracy, and reduces false alarms, making the Hybrid Model more robust and efficient for modern network security environments.

Table 1: Performance Metrics

S.No	Metric	Signature-Based	Anomaly-Based	Hybrid Model
1	Accuracy	91%	93%	97%
2	False Positive Rate	6%	8%	3%
3	Detection Rate	89%	94%	98%

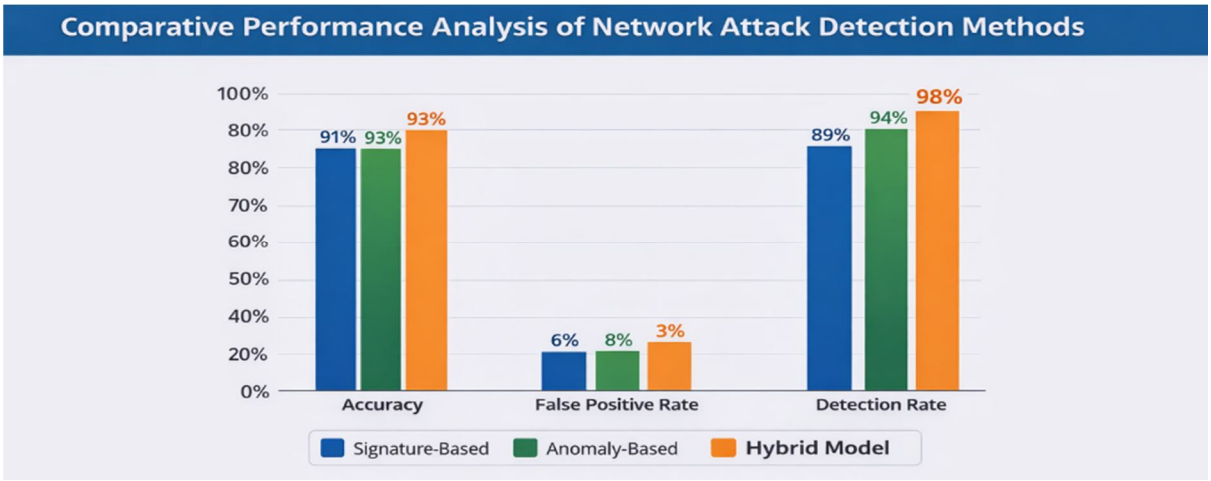


Figure 2: Comparative analysis

Figure 2 shows that a comparative performance analysis of three network attack detection approaches: Signature-Based, Anomaly-Based, and Hybrid Model, evaluated using Accuracy, False Positive Rate, and Detection Rate. From the Accuracy metric, the Hybrid Model achieves the highest value at 97%, compared to 93% for the Anomaly-Based model and 91% for the Signature-Based method. This indicates that integrating both detection techniques significantly improves the overall correctness of classification. In terms of False Positive Rate, the Hybrid Model records the lowest percentage at 3%, whereas the Signature-Based and Anomaly-Based approaches show 6% and 8% respectively. A lower false positive rate means fewer legitimate network activities are incorrectly flagged as attacks, reducing unnecessary alerts and improving operational efficiency. For Detection Rate, the Hybrid Model again outperforms the other two methods with 98%, followed by Anomaly-Based at 94% and Signature-Based at 89%. This demonstrates that the hybrid system is more effective in identifying actual attack instances, including both known and unknown threats. Overall, the chart clearly shows that the Hybrid Model combines the strengths of signature-based precision and anomaly-based adaptability, resulting in higher accuracy, improved detection capability, and reduced false alarms.

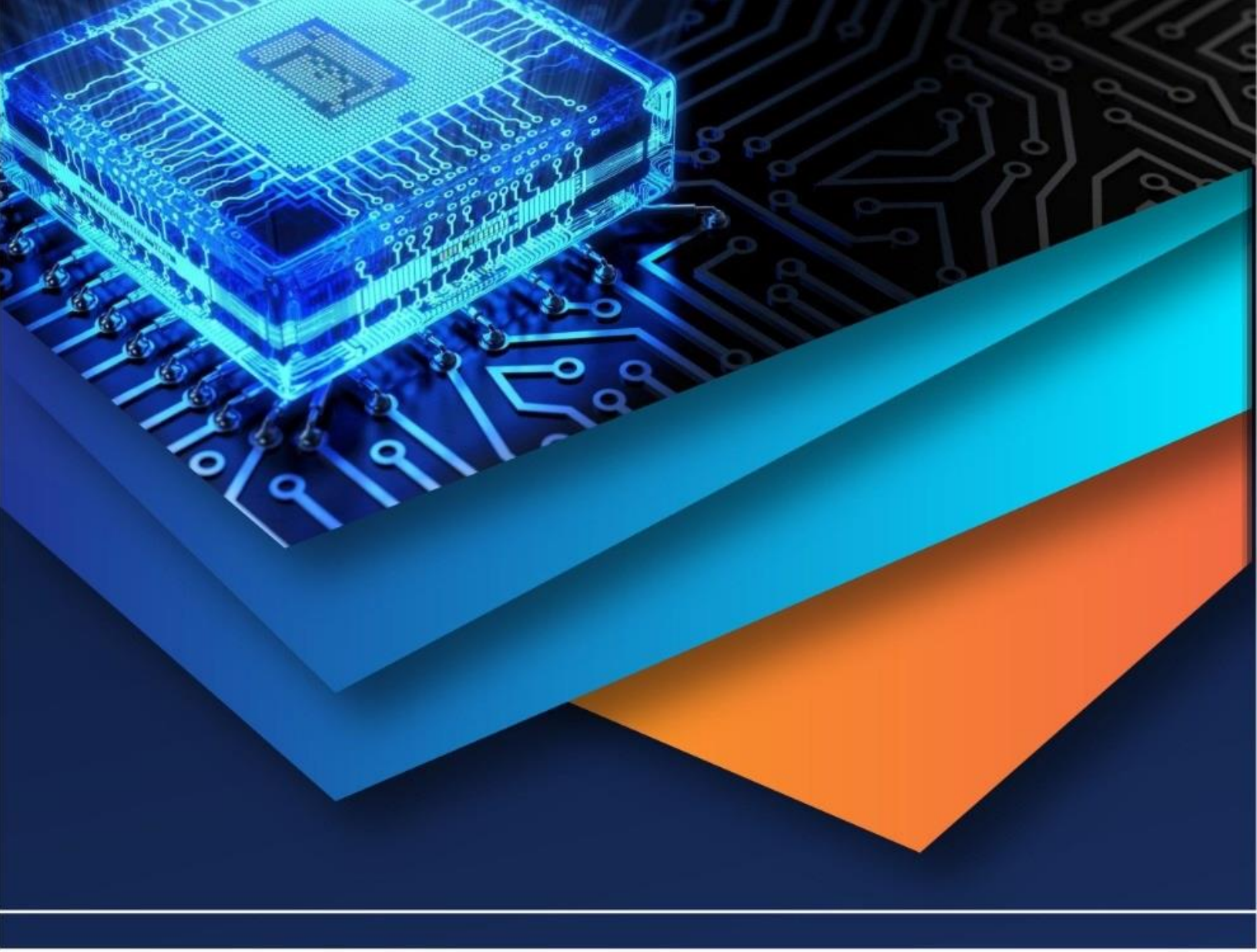
VI. CONCLUSION

The comparative analysis of Signature-Based, Anomaly-Based, and Hybrid detection approaches clearly demonstrates that the Hybrid Model provides superior performance in network attack detection. By integrating signature matching for known threats with anomaly detection for unknown and zero-day attacks, the hybrid approach achieves higher accuracy and detection rates while significantly reducing false positives.

The results indicate that standalone methods have inherent limitations, either in detecting new threats or in generating excessive false alarms. The hybrid framework effectively overcomes these weaknesses by combining precision and adaptability within a unified architecture. Furthermore, the reduced false positive rate enhances operational efficiency and minimizes unnecessary administrative intervention. Overall, the Hybrid Anomaly and Signature-Based Approach offers a robust, scalable, and reliable solution for securing modern network environments against evolving cyber threats.

REFERENCES

[1] J. Huang, Z. Chen, S.-Z. Liu, H. Zhang and H.-X. Long, "Improved Intrusion Detection Based on Hybrid Deep Learning Models and Federated Learning," IEEE Access, vol. 12, pp. 102345–102358, 2024, doi: 10.1109/ACCESS.2024.3398765.
[2] S. Sadhwani, R. Patel and M. Sharma, "A Hybrid CNN–BiLSTM Model for Intrusion Detection in IoT Networks," IEEE Internet of Things Journal, vol. 12, no. 3, pp. 2156–2168, 2025, doi: 10.1109/JIOT.2025.3456789.
[3] A. G. Ayad, N. A. Sakr and N. A. Hikal, "A Hybrid Approach for Efficient Feature Selection in Anomaly Intrusion Detection for IoT Networks," IEEE Access, vol. 12, pp. 56789–56802, 2024, doi: 10.1109/ACCESS.2024.3365432.
[4] L. G. Aldawood, Z. M. Jiwar, E. A. Hadi, M. A. Al-Shareeda and M. Almaayah, "A Hybrid Anomaly–Rule–Pattern Detection Framework for Streaming-Based Persistent Intrusion Detection," IEEE Systems Journal, vol. 19, no. 1, pp. 455–466, 2025, doi: 10.1109/JSYST.2025.3478912.
[5] S. Alharbi and A. Khan, "Ensemble Defense System: A Hybrid IDS Approach for Effective Cyber Threat Detection," IEEE Access, vol. 12, pp. 78901–78915, 2024, doi: 10.1109/ACCESS.2024.3345678.
[6] R. Baidar, S. Maric and R. Abbas, "Hybrid Deep Learning–Federated Learning Powered Intrusion Detection System for IoT/5G Advanced Edge Computing Network," IEEE Transactions on Network and Service Management, vol. 22, no. 2, pp. 1345–1358, 2025, doi: 10.1109/TNSM.2025.3489123.
[7] J. Manikandan and U. Srilakshmi, "Deep Learning-Based Vulnerability Detection and Mitigation in Virtualization Data Center," International Journal of Maritime Engineering, vol. 1, pp. 647–662, 2024, doi: 10.5750/ijme.v1i1.1393.
[8] J. Manikandan and U. Srilakshmi, "HMM-Assisted Proactive Vulnerability Mitigation in Virtualization Datacenter Through Controlled VM Placement," in Proceedings of Springer Conference, 2023, doi: 10.1007/978-981-19-7615-5_32.
[9] J. Manikandan, V. Vemulapalli, K. Spandana, S. Vikruthi, B. Lakshmikanth and M. Radhika, "Studying the Linear Degree of Community Network Patterns to Eliminate Misclassification Trouble the Use of Gaining Knowledge Approaches," in 2025 International Conference on Computing Technologies (ICOCT), Bengaluru, India, 2025, pp. 1–5, doi: 10.1109/ICOCT64433.2025.11118921.
[10] S. Badonia, M. V. Babu, N. R. Lakkimsetty, G. Kavitha and A. P. N, "Implication and Challenges in Modernisation of Healthcare System using 5G," in 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N), Greater Noida, India, 2024, pp. 834–837, doi: 10.1109/ICAC2N63387.2024.10894954.
[11] R. Shaik, M. V. Babu, S. Medichelimi, C. Paritala, A. Amaranayani and I. Narasimharao, "Physical Layer Security for WSNs: Addressing Eavesdropping and Energy Constraints," in 2025 7th International Conference on Inventive Material Science and Applications (ICIMA), Namakkal, India, 2025, pp. 27–32, doi: 10.1109/ICIMA64861.2025.11074037.
[12] K. Pande, V. Babu, V. Tripathi, P. K, N. Bhatt and Manjuvani, "Dynamic Security and Efficiency Improvements in IoT Through Enhanced Security Bounds Framework," in 2025 2nd International Conference On Multidisciplinary Research and Innovations in Engineering (MRIE), Gurugram, India, 2025, pp. 562–566, doi: 10.1109/MRIE66930.2025.11156654.
[13] P. V. Reddy, D. Ganesh, S. Reddy Gaddam, C. Swarna Lalitha, S. Muqthadar Ali and K. Sakibaev, "Empirical Assessment of Profit Predicting Deep Learning Methods," in 2025 5th International Conference on Soft Computing for Security Applications (ICSCSA), Salem, India, 2025, pp. 1674–1679, doi: 10.1109/ICSCSA66339.2025.11171150.
[14] Y. K. Gupta, S. Reddy Gaddam, H. Gupta and S. Banerjee, "An Optimized Swarm Intelligence Approach for Fuzzy Clustering-Based Intrusive Behavior Detection in IoT and Network System," in 2025 IEEE Madhya Pradesh Section Conference (MPCON), Jabalpur, India, 2025, pp. 864–870, doi: 10.1109/MPCON66082.2025.11256633.
[15] R. Sahith, S. Reddy Gaddam, P. V. Reddy, D. Ganesh, G. Varma Kosuri and K. L. Thanukula, "Ultrasonic Bioacoustics and Deep Learning for Early Plant Disease Prediction," in 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2025, pp. 1713–1718, doi: 10.1109/ICSCDS65426.2025.11167734.
[16] S. Vikruthi, M. S. Suneetha, P. Hussain Basha, B. Sreelekha, B. Bruhati and M. Asmitha, "Design and Development of IoT Based Smart Women Security Gadget," in 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India, 2023, pp. 1747–1753, doi: 10.1109/ICSCNA58489.2023.10370638.
[17] S. Vikruthi, T. R. Singasani, V. T. R. P. K. M, P. V. V. S. D. Nagendrudu, C. Raghavendra and R. Sahith, "Detection of Emergency Vehicles in Traffic and Assign Traffic Free Path Using Deep Learning," in 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2025, pp. 1252–1261, doi: 10.1109/ICSADL65848.2025.10933032.
[18] Mr Sasidhar Reddy Gaddam and DOI : 10.48047/IJCNIS.14.3.1283, "Java-Driven Trustworthy And Reliable Deep Learning For Cyberattack Detection In Industrial Iot", Int. j. commun. netw. inf. secur., vol. 14, no. 3, pp. 1274–1283, Apr. 2022.
[19] V. Babu, V. Ramya, and V. S. Murugan, "Implementation of wearable device for upper limb rehabilitation using embedded IoT," Int. J. Electron. Signals Syst. Manag. Sci., vol. 16, no. 1, pp. 90–95, Mar. 2024. [Online]. Available: https://doi.org/10.1504/IJESMS.2024.136972
[20] M. V. . Babu, V. . Ramya, and V. S. . Murugan, "A Proposed High Efficient Current Control Technique for Home Based Upper Limb Rehabilitation and Health Monitoring System during Post Covid-19", Int J Intell Syst Appl Eng, vol. 12, no. 2s, pp. 600–607, Oct. 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY