Journal of Theoretical and Applied Information Technology
31st October 2026. Vol.104. No.20
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ADAPTIVE CYBER-RESILIENCE FRAMEWORK FOR INTELLIGENT INTRUSION DETECTION IN 6G-ENABLED INTERNET OF MEDICAL THINGS NETWORKS

BASIL BABY K[1], Dr. A. NITHYA RANI[2]
[1]PhD Research Scholar, Affiliation, CMS College Of Science and Commerce, Chinnavedampatti, Coimbatore, India
[2]Associate Professor, CMS College Of Science And Commerce, Chinnavedampatti, Coimbatore, India
E-mail: [1]mail4basilbaby@gmail.com, [2]nithyarani.a@gmail.com

ABSTRACT

Network security has become increasingly critical in 6G-enabled Internet of Medical Things (IoMT) networks, where massive device connectivity, heterogeneous communication, and low-latency healthcare services expand the potential attack surface. The resource-constrained and sensitive nature of IoMT requires intrusion detection mechanisms that are adaptive, resilient, and computationally efficient. Network Intrusion Detection Systems (NIDS) provide an essential layer of protection by monitoring network traffic and identifying anomalous activities and potential attacks. This study proposes an Adaptive Cyber-Resilience Framework that integrates bio-inspired optimization with adaptive anomaly detection, dynamic rule adjustment, automated response, and continuous feedback to strengthen NIDS performance. Experimental evaluation using a network intrusion dataset demonstrates that the proposed framework achieves 77.512% detection accuracy, 77.941% F-measure, 79.698% precision, and 76.259% recall, outperforming DI-NIDS and DMAN. The framework also achieves an attack detection rate of 76.259% and a missed detection rate of 23.741%, demonstrating its potential to provide adaptive and resilient intrusion detection for next-generation IoMT networks.

Keywords: *Network Intrusion Detection Systems, 6G, Internet of Medical Things, Intrusion Detection, Cybersecurity in Healthcare, Oranguttan Optimization.*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have become a cornerstone of modern communication systems, enabling the seamless collection, processing, and transmission of data in a distributed manner [1]. These networks consist of spatially dispersed sensor nodes that monitor physical or environmental conditions such as temperature, pressure, or motion. WSNs are widely deployed in diverse fields, including environmental monitoring, healthcare, military surveillance, and smart cities [2]. Despite their versatility, the resource-constrained nature of WSNs, including limited energy, computational power, and storage, makes them susceptible to various security vulnerabilities. These vulnerabilities often serve as entry points for malicious actors aiming to compromise the network's integrity, confidentiality, and availability [3].

The evolution of WSNs has led to the emergence of the Internet of Medical Things (IoMT), a specialized domain that integrates medical devices and sensors into interconnected systems for healthcare monitoring and management. IoMT leverages WSNs to enable real-time tracking of patient health metrics, remote diagnostics, and precision medicine. Applications of IoMT include wearable devices, implantable sensors, and smart diagnostic equipment, all of which generate vast amounts of sensitive data [4]. While IoMT offers unparalleled advancements in healthcare, it also inherits the security challenges of WSNs. The inclusion of medical data, which is highly confidential and critical, further elevates the risks posed by potential intrusions [5].

Intrusion detection in IoMT has emerged as a critical component in addressing these security challenges. Intrusions refer to unauthorized access or malicious activities that disrupt the normal operation of a network [6]. In IoMT, such intrusions can compromise patient data privacy, tamper with medical devices, or disrupt the overall functioning of healthcare systems, potentially endangering lives. The complexity of IoMT networks, combined with their resource constraints and mobility, demands advanced methods for detecting and mitigating intrusions effectively [7]. Traditional security measures such as firewalls and encryption, while essential, are often insufficient to detect

internal threats or advanced attacks, necessitating the use of specialized intrusion detection systems (IDS[8]).

Network-based Intrusion Detection Systems (NIDS) have gained prominence as a robust solution for securing IoMT networks. Unlike host-based intrusion detection systems, which monitor individual devices, NIDS analyze network traffic to identify suspicious patterns or anomalies [9]. This approach is particularly suited for IoMT, where multiple devices communicate over shared networks, making centralized monitoring both practical and effective. NIDS operate by capturing data packets transmitted across the network and applying predefined rules or machine learning algorithms to detect potential threats. These systems are capable of identifying various forms of intrusions, including denial-of-service attacks, unauthorized access, data exfiltration, and protocol-based exploits [10].

The role of NIDS in intrusion detection for IoMT is multifaceted. First, NIDS provide real-time monitoring of network traffic, enabling the early detection of anomalies that may indicate a security breach. By analyzing packet headers, payloads, and communication patterns, NIDS can identify deviations from expected behavior, such as unusual data transmission rates or unauthorized connections [11]. This capability is crucial for IoMT networks, where time-sensitive data transmissions are critical for patient care. Second, NIDS enhance the overall security posture of IoMT by integrating with other defense mechanisms such as firewalls and encryption protocols. This layered security approach ensures comprehensive protection against both external and internal threats [12].

NIDS in IoMT also address the challenges posed by the heterogeneity of devices and communication protocols. IoMT networks often comprise a diverse array of sensors, actuators, and gateways, each with its own communication standards and operational requirements [13]. NIDS bridge this heterogeneity by providing a unified framework for monitoring and analyzing network traffic, regardless of the underlying protocols. Furthermore, NIDS can adapt to the dynamic nature of IoMT, where devices frequently join or leave the network, by employing techniques such as anomaly detection and behavioral profiling to maintain security [14].

Another critical aspect of NIDS in IoMT is the ability to mitigate false positives and false negatives. False positives, where legitimate traffic is incorrectly flagged as malicious, can disrupt normal operations, while false negatives, where malicious activities go undetected, can lead to severe consequences [15]. NIDS employ advanced detection methods such as signature-based detection, anomaly-based detection, and hybrid approaches to minimize these errors. Signature-based detection uses predefined attack signatures to identify known threats, while anomaly-based detection establishes a baseline of normal behavior and flags deviations. Hybrid approaches combine the strengths of both methods, offering a balanced solution for IoMT security [16].

Scalability and resource efficiency are additional considerations for NIDS in IoMT. Given the limited computational and energy resources of IoMT devices, NIDS must be lightweight and optimized to operate effectively without overburdening the network. Techniques such as distributed intrusion detection, where monitoring responsibilities are shared among multiple nodes, and edge computing, which processes data closer to its source, enhance the scalability and efficiency of NIDS [17]. These advancements ensure that NIDS can secure IoMT networks even as they expand in size and complexity.

Incorporating feedback mechanisms further elevates the effectiveness of NIDS in IoMT. By continuously learning from detected intrusions and adapting detection rules, NIDS improve their accuracy and responsiveness over time. This adaptive capability is essential for addressing the evolving threat landscape, where attackers constantly develop new methods to bypass security measures [18]. Feedback-driven NIDS integrate seamlessly into the IoMT ecosystem, providing proactive and resilient security that aligns with the dynamic nature of modern healthcare systems.

The transition toward sixth-generation (6G) wireless communication is expected to further expand IoMT through ultra-low-latency communication, massive device connectivity, and intelligent healthcare services. However, the growing heterogeneity and connectivity of 6G-enabled IoMT can increase the attack surface and expose healthcare networks to evolving cyber threats. Adaptive and resilient intrusion detection mechanisms are therefore essential for maintaining secure communication and reliable healthcare services in next-generation IoMT environments.

1.1 Problem Statement and Research Questions

Despite advances in network intrusion detection, existing approaches continue to face challenges in balancing detection performance, adaptability, and computational efficiency in dynamic and resource-constrained Internet of Medical Things (IoMT) environments. Signature-based detection remains dependent on known attack patterns, while anomaly-based approaches may generate false alarms when legitimate network behaviour changes. Existing studies, including DI-NIDS [28] and DMAN [9], address domain variation and minority-attack detection, respectively, but the reviewed literature indicates a need to investigate a coordinated framework that integrates adaptive resource allocation, signature prioritization, contextual anomaly detection, dynamic rule adjustment, automated response, and continuous feedback. The research problem addressed in this study is the development and evaluation of an integrated intrusion detection framework that improves classification performance and attack detection while reducing missed detections. Accordingly, the study proposes Orangutan-Enhanced Network Defense (OEND) and evaluates its performance against DI-NIDS and DMAN using classification accuracy, F-measure, precision, recall, attack detection rate, and missed detection rate.

The following research questions guide the investigation:

RQ1: Does the proposed OEND framework achieve better classification accuracy, F-measure, precision, and recall than DI-NIDS and DMAN on the selected intrusion detection dataset?

RQ2: To what extent does OEND improve attack detection and reduce missed detections compared with the selected baseline methods?

RQ3: How does the integration of adaptive resource allocation, signature prioritization, contextual anomaly detection, dynamic rule adjustment, automated response, and continuous feedback contribute to the proposed framework's intrusion detection process?

1.2 Motivation and Objective

The rapid expansion of IoMT has revolutionized healthcare by enabling real-time monitoring and advanced diagnostics. This progress, however, has introduced critical vulnerabilities, as IoMT networks carry highly sensitive medical data and control vital devices. The motivation stems from the need to secure these networks against increasing cyber threats, including unauthorized access, data breaches, and operational disruptions. Ensuring patient safety and data integrity necessitates robust intrusion detection mechanisms. The objective focuses on developing an efficient NIDS framework tailored to IoMT's dynamic and resource-constrained environments. This includes designing adaptive detection methods that address the unique challenges of IoMT, such as device heterogeneity, encrypted traffic, and evolving threats, while maintaining low latency and minimal resource consumption.

1.3 Research Gap

Existing intrusion detection systems often fall short in addressing the specific needs of IoMT environments. Traditional NIDS frameworks primarily cater to conventional networks and lack the adaptability required for IoMT's dynamic and heterogeneous nature. Many current solutions struggle to balance accuracy with the limited computational and energy resources of IoMT devices. Approaches relying heavily on signature-based detection face challenges in identifying zero-day attacks, while anomaly-based methods frequently suffer from high false positive rates. Encrypted traffic analysis remains underexplored, leaving gaps in detecting hidden threats. Furthermore, the integration of lightweight, scalable, and feedback-driven NIDS solutions tailored for IoMT networks is still in its infancy, emphasizing the need for targeted research to bridge these critical gaps.

1.4 Research Hypothesis

H1 (Alternative Hypothesis): The proposed Orangutan-Enhanced Network Defense (OEND) framework achieves higher classification accuracy, F-measure, precision, recall, and attack detection rate, together with a lower missed detection rate, than DI-NIDS and DMAN on the selected network intrusion detection dataset.

H0 (Null Hypothesis): The proposed OEND framework does not demonstrate superior performance over DI-NIDS and DMAN across the specified intrusion detection metrics on the selected dataset.

2. LITERATURE REVIEW

"MLP-GWO" [19] explores the integration of Gray Wolf Optimization (GWO) with a multilayer perceptron (MLP) for network intrusion detection. It focuses on enhancing the training efficiency and performance of MLP by employing GWO as an

optimization technique. The study examines the theoretical implications of leveraging bio-inspired algorithms to improve the detection capabilities of intrusion detection systems (IDS), emphasizing scalability and adaptability in dynamic network environments. "CNN-IDS" [20] investigates the application of synaptic intelligent convolutional neural networks (CNN) for intrusion detection in dynamic IoT environments. It explores the theoretical aspects of CNN-based architectures tailored for real-time IoT security. The research highlights the importance of adaptive learning mechanisms and intelligent feature extraction in addressing IoT-specific challenges, contributing to advancements in IoT security frameworks. "SPB-IDS" [21] examines the use of Sandpiper Optimization combined with a hybrid deep learning model for intrusion detection in blockchain-enabled IoT environments. It focuses on the theoretical integration of optimization algorithms with deep learning to enhance intrusion detection accuracy and efficiency. The study emphasizes the unique role of blockchain in securing IoT networks, contributing to the development of advanced security solutions.

"MultiBinary-IDS" [22] investigates the application of multi-binary classifiers with optimal feature selection techniques for intrusion detection. It focuses on designing memory-efficient IDS suitable for resource-constrained environments. The study explores theoretical approaches for reducing computational overhead while maintaining high detection accuracy, providing a framework for scalable and efficient intrusion detection systems. "GRU-IDS-Swarm" [23] explores the application of GRU-based intrusion detection systems for IoT environments, enhanced with swarm optimization and Gaussian Random Forest classification. It examines theoretical methods for integrating recurrent neural networks with bio-inspired optimization and ensemble learning techniques. The research highlights the potential of hybrid models in addressing IoT-specific intrusion detection challenges, contributing to robust security solutions. "GAN-OneClass-NIDS" [24] investigates the application of Generative Adversarial Networks (GAN) as a one-class classifier for early detection of network intrusions. It focuses on the theoretical implications of using GANs for anomaly detection in network traffic, highlighting their ability to model normal behavior and identify deviations. The research contributes to enhancing proactive intrusion detection capabilities, emphasizing early threat identification in network security systems.

"FeatureImage-ViT-NIDS" [25] explores the use of feature images and deformable Vision Transformers (ViT) for network intrusion detection. It examines the theoretical integration of computer vision techniques with intrusion detection models, focusing on feature extraction and transformation. The study highlights the potential of using image-based representations and advanced transformer architectures to improve detection accuracy in NIDS, contributing to novel approaches in cybersecurity. "Fusional-Hierarchical-IDS" [26] presents a fusional intrusion detection method that integrates hierarchical filtering with a progressive detection model. The theoretical study focuses on the fusion of multiple detection techniques to enhance accuracy and reduce false positives. It emphasizes the importance of hierarchical and progressive approaches in building robust and adaptive NIDS, contributing to improved network security frameworks. "CNN-BiLSTM" [27] examines a network intrusion detection method that combines CNN, Bidirectional Long Short-Term Memory (BiLSTM), and an attention mechanism. It explores the theoretical integration of these components to enhance feature extraction, sequential learning, and focus on critical patterns in network data. The research highlights the effectiveness of hybrid deep learning models in improving intrusion detection capabilities.

"DI-NIDS" [28] investigates a domain-invariant approach to network intrusion detection, focusing on adaptability across varying network environments. It explores the theoretical foundations of achieving domain invariance in IDS to enhance their applicability and performance. The study emphasizes the integration of innovative techniques to address challenges posed by domain shifts and inconsistencies in network traffic. By delving into architectural and algorithmic considerations, it contributes to advancing the field of network security and IDS development, ensuring robust intrusion detection across diverse domains.

"DMAN" [9] examines an effective methodology for detecting minority attacks in NIDS by leveraging deep learning and advanced sampling techniques. It focuses on addressing the imbalance in attack detection, highlighting the importance of minority class recognition. The paper emphasizes the theoretical aspects of combining deep learning models with data sampling strategies to improve

detection accuracy for underrepresented attack patterns. This exploration provides a foundation for enhancing NIDS capabilities, especially in handling imbalanced datasets and ensuring comprehensive intrusion detection.

2.1 Critical Synthesis of Existing Intrusion Detection Approaches

The reviewed studies demonstrate several complementary strategies for improving network intrusion detection. MLP-GWO [19] and SPB-IDS [21] integrate bio-inspired optimization with learning-based detection, whereas CNN-IDS [20], GRU-IDS-Swarm [23], and CNN-BiLSTM [27] emphasize feature extraction and the analysis of network traffic patterns. MultiBinary-IDS [22] focuses on feature selection and memory efficiency, while GAN-OneClass-NIDS [24] explores anomaly detection by modelling normal traffic behaviour. FeatureImage-ViT-NIDS [25] investigates image-based feature representations, and Fusional-Hierarchical-IDS [26] adopts hierarchical detection. DI-NIDS [28] addresses domain variation, whereas DMAN [9] focuses on detecting minority attack classes through deep learning and sampling strategies.

Despite these contributions, the reviewed approaches target different aspects of intrusion detection, and their descriptions do not establish whether the approaches jointly integrate adaptive resource allocation, signature prioritization, contextual anomaly analysis, dynamic rule adjustment, automated response, and continuous feedback within a unified framework. The literature descriptions also provide insufficient consistent evidence to determine whether the approaches have been evaluated using comparable datasets, experimental settings, and performance measures. Consequently, their relative effectiveness in balancing detection performance, adaptability, and operational efficiency in resource-constrained Internet of Medical Things environments remains insufficiently established by the literature reviewed here.

The proposed Orangutan-Enhanced Network Defense (OEND) framework addresses this integration gap by organizing environment scanning, adaptive resource allocation, signature library prioritization, real-time anomaly detection, suspicious-pattern clustering, behavioural analysis, dynamic rule adjustment, automated response, and continuous learning into a coordinated detection process. Its comparative evaluation against DI-NIDS [28] and DMAN [9] examines classification accuracy, F-measure, precision, recall, attack detection rate, and missed detection rate. The intended distinction lies in integrating detection, adaptation, and response mechanisms within a single framework rather than relying on an individual technique alone. Nevertheless, the extent to which OEND reduces computational overhead, supports real-time operation, or generalizes to actual 6G-enabled IoMT deployments requires separate empirical validation.

2.2 Distinction of the Proposed OEND Framework from Existing Studies

The proposed Orangutan-Enhanced Network Defense (OEND) framework differs from the reviewed intrusion detection approaches primarily in its coordinated, multi-stage design. MLP-GWO [19] focuses on optimization-assisted neural network training, CNN-IDS [20] emphasizes convolution-based feature learning, SPB-IDS [21] combines optimization with deep learning for blockchain-enabled IoT security, and GRU-IDS-Swarm [23] explores recurrent learning with swarm optimization and ensemble classification. GAN-OneClass-NIDS [24] addresses anomaly detection, FeatureImage-ViT-NIDS [25] investigates feature-image representation with Vision Transformers, and CNN-BiLSTM [27] combines spatial feature extraction with sequential learning. DI-NIDS [28] focuses on domain-invariant detection, whereas DMAN [9] targets minority-attack detection. In contrast, OEND organizes environment scanning, adaptive resource allocation, signature library prioritization, real-time anomaly detection, suspicious-pattern clustering, behavioural analysis and contextual awareness, dynamic rule adjustment, automated response, and continuous learning and feedback integration into a single framework. The study further compares OEND with DI-NIDS and DMAN using classification accuracy, F-measure, precision, recall, attack detection rate, and missed detection rate. The reported results show an accuracy of 77.512%, an F-measure of 77.941%, precision of 79.698%, recall of 76.259%, an attack detection rate of 76.259%, and a missed detection rate of 23.741% for OEND on the selected dataset. The principal distinction is thus the integration of detection, adaptation, response, and feedback mechanisms, together with a comparative evaluation using multiple performance metrics. Since the evaluation uses a general network intrusion detection dataset, the results do not independently establish effectiveness in real-world 6G-enabled IoMT environments; domain-specific

validation remains an important direction for further study.

Recent research has investigated diverse approaches to intelligent network analysis, cybersecurity, optimization, and adaptive communication. Graph-based learning and network-flow analysis have been explored for trust management and scalable digital identity systems [29], [30], while optimization-assisted classification has been investigated for software defect prediction and intrusion detection [33], [35], [36]. Cybersecurity research has also examined adversarial threats in IoT environments [40], machine-learning-based cybercrime analysis [43], and security awareness [54]. Related studies address secure data sharing through identity-based encryption [55] and intelligent methods for improving energy efficiency in smart cities [34]. Research on advanced communication systems has examined AI-driven energy-efficient 6G connectivity [37], adaptive beamforming [38], and real-time 6G applications [39]. Intelligent optimization and learning have also been applied to sentiment classification [31], [41], [42], medical classification [45], [49], and computational modelling [44], [47]. Although these studies contribute to their respective research domains, the present work specifically investigates intrusion detection through the proposed Orangutan-Enhanced Network Defense (OEND) framework. The framework coordinates environment scanning, adaptive resource allocation, signature library prioritization, anomaly detection, behavioural analysis, dynamic rule adjustment, automated response, and continuous feedback. The central research focus is the integration of these functions into a coordinated detection process and the comparative assessment of detection performance against DI-NIDS and DMAN.

Further studies have investigated intelligent optimization and adaptive mechanisms for network reliability, resource management, and emerging computational environments. Graph neural networks and reinforcement learning have been applied to urban traffic optimization [46], while distributed-system approaches have been examined for metaverse applications [32]. Research on intelligent routing and network optimization has addressed reliability and packet loss in drone ad-hoc networks [48], quality of service and energy efficiency [50], and ultra-low-latency communication in 6G drone networks [57], [59]. Related work has considered energy-efficient quantum wireless sensor networks [51], blockchain-supported communication in heterogeneous wireless sensor networks [52], and safety-oriented queuing models for quantum drone networks [53]. Other studies have explored AI-driven sustainability in business management [56] and mathematical representations based on plithogenic structures [58]. These contributions provide broader context for understanding optimization, resource utilization, intelligent decision-making, and security across networked systems. Nevertheless, routing optimization, mathematical modelling, and application-specific classification differ from the intrusion detection objective addressed in the present study. OEND focuses on coordinating detection, adaptation, response, and feedback mechanisms, with performance assessed through classification accuracy, precision, recall, F-measure, attack detection rate, and missed detection rate. Since the evaluation uses a general network intrusion detection dataset, further validation using healthcare-specific traffic and representative 6G-enabled Internet of Medical Things environments is required to establish practical applicability and generalizability.

3. ORANGUTAN-ENHANCED NETWORK DEFENSE (OEND)

"Orangutan-Enhanced Network Defense (OEND)" introduces an innovative optimization approach for NIDS inspired by the adaptive behaviour of orangutans in their natural habitat. Orangutans exhibit strategic planning, efficient resource utilization, and the ability to make quick decisions, which aligns well with the requirements of modern intrusion detection. By modelling the intelligence and decision-making traits of orangutans, OEND provides a structured nine-step framework that enhances the performance of NIDS, allowing for more accurate and faster intrusion detection.

3.1 Environment Scanning in OEND

Environment Scanning, the foundational phase in the OEND optimization framework. In this phase, NIDS captures and assesses network traffic to establish a baseline that identifies standard patterns within the network. These patterns serve as a reference for recognizing abnormal activity that may indicate an intrusion. By focusing on understanding the network's operational state, this phase effectively supports the succeeding steps in OEND, where anomaly detection and adaptive responses rely on the initial analysis provided here. This step uses mathematical formulations to quantify and characterize various aspects of

network traffic, ensuring a precise and reliable baseline.

Network Traffic Volume Calculation

To monitor traffic effectively, it is crucial to understand network volume at any given time. Traffic volume represents the total data packets transmitted within a specific time interval across a network. The formula to calculate traffic volume V is represented mathematically in Eq.(1).

$$V = \sum_{i=1}^{n} P_i \quad (1)$$

where P_i indicates the size of each packet in bytes, and n represents the total number of packets within the designated time interval. By determining V, NIDS can understand the network's average traffic volume, which will aid in spotting sudden spikes or drops that may signify abnormal activity. Monitoring this parameter allows NIDS to distinguish typical fluctuations from potential intrusions, establishing a solid foundation for anomaly detection.

Traffic Flow Rate Measurement

Calculating the traffic flow rate becomes essential to analyze the speed at which data flows through the network. Traffic flow rate F can be determined mathematically in Eq.(2).

$$F = \frac{V}{T} \quad (2)$$

where V stands for traffic volume as calculated previously, and T denotes the time interval over which V is measured. This rate captures the dynamic aspects of network traffic, providing NIDS with critical information on data transmission speed across the network. By tracking fluctuations in F, Environment Scanning can detect unusual patterns that might signify potential threats. Changes in flow rate serve as indicators of altered network behaviour, highlighting shifts that warrant closer inspection in later steps. T is vital as it defines the observation period for monitoring traffic volume. Typically measured in seconds, T sets the timeframe within which NIDS captures and assesses network traffic. Monitoring F indicates regular flow rates, with deviations alerting the system to possible network events that require attention. These calculations give NIDS a quantitative view of regular network activity, enabling precise anomaly detection.

Packet Size Distribution Analysis

Analyzing the distribution of packet sizes is another essential aspect of Environment Scanning. Packet size distribution provides information on the range of packet sizes typically found within the network, assisting NIDS in identifying deviations that may indicate attacks. This distribution can be mathematically represented in Eq.(3) as the probability distribution function $P(s)$.

$$P(s) = \frac{N(s)}{N_{total}} \quad (3)$$

where $N(s)$ represents the number of packets of size s, and N_{total} stands for the total number of packets observed. This distribution function helps determine the likelihood of encountering various packet sizes within the network, establishing an expected range of values. Abnormal packet sizes detected later can be compared against this distribution to identify patterns that deviate from the norm.

Data Packet Rate Calculation

The packet rate, an essential network activity indicator, quantifies the number of packets transmitted within a specific period. This metric is crucial for identifying sudden increases in traffic volume that may correspond to unauthorized access attempts or Distributed Denial of Service (DDoS) attacks. The packet rate R_p is calculated as shown in Eq.(4).

$$R_p = \frac{n}{T} \quad (4)$$

where n represents the number of packets within the time interval T. By measuring R_p, Environment Scanning defines a baseline rate, highlighting sudden deviations that may signal abnormal activity or attacks. Monitoring real-time packet rates enhances NIDS's capacity to respond swiftly to unexpected traffic surges.

Bandwidth Utilization Estimation

Bandwidth utilization, representing the percentage of available network capacity used over a specific period, is a crucial metric within Environment Scanning. Bandwidth utilization U can be calculated as expressed mathematically in Eq.(5).

$$U = \frac{V}{B} \times 100 \quad (5)$$

where V denotes the total traffic volume observed, and B represents the maximum bandwidth capacity

of the network. By calculating U, NIDS establishes the degree of network usage, identifying potential bandwidth anomalies that might suggest malicious activities. High utilization can indicate abnormal network congestion, prompting further analysis in later stages.

3.2 Adaptive Resource Allocation in OEND

Adaptive Resource Allocation maximizes NIDS efficiency by strategically allocating computational resources based on dynamic network demands. Inspired by orangutans' resourcefulness and ability to allocate energy according to situational requirements, Adaptive Resource Allocation in OEND dynamically redistributes resources to optimize the detection and analysis processes. This phase takes the insights from Environment Scanning and adjusts the computational workload by prioritizing high-traffic times or critical alerts, ensuring an energy-efficient, responsive approach to intrusion detection. Critical calculations help monitor and adapt resource distribution according to traffic volume, system capacity, and bandwidth Availability.

Computational Load Calculation

The computational load directly influences NIDS efficiency. Calculating computational load C_L provides an understanding of the processing demand based on network traffic and system capacity. The equation for computational load C_L is expressed mathematically in Eq.(6).

$$C_L = \frac{P \times T}{C} \tag{6}$$

where P represents the total number of packets processed, T indicates the processing time in seconds, and C denotes the system's computational capacity. By monitoring C_L, NIDS can dynamically assess its current load, redistributing resources effectively based on fluctuations in network traffic or peak usage periods. This adaptive capability ensures that the system remains efficient while handling variable demands.

Dynamic Buffer Allocation

To manage high traffic effectively, adaptive buffer allocation becomes essential. Dynamic buffer size B_S allocation enhances NIDS performance by adjusting buffer space based on packet load. The formula for dynamic buffer allocation B_S is expressed mathematically in Eq.(7).

$$B_S = \frac{R_P \times \Delta T}{K} \tag{7}$$

where R_P represents the packet rate, ΔT is the interval of buffer reallocation, and K is a scaling factor that adapts the buffer size to the current load. Dynamic buffer allocation prevents packet overflow during high-traffic periods, which would otherwise lead to packet loss or delayed response in detecting intrusions. This step aligns with orangutan behaviour in managing limited resources efficiently to handle sudden needs.

Processor Utilization Rate

Optimal processor utilization is critical in NIDS operations, as it affects the speed and accuracy of detection. The processor utilization rate U_P measures the percentage of computational resources used relative to total system capacity. Processor utilization can be calculated as expressed in Eq.(8).

$$U_P = \frac{C_L}{C} \times 100 \tag{8}$$

where C_L denotes the computational load calculated previously, and C refers to the maximum system capacity. Calculating U_P gives insights into system efficiency, allowing resource adjustments to avoid overload. Adaptive changes based on U_P prevent scenarios where high processing demand compromises system performance, ensuring continuous, effective monitoring of potential threats.

Dynamic Bandwidth Allocation

The distribution of available bandwidth greatly influences NIDS performance, especially when handling varying data volumes. Dynamic bandwidth allocation adjusts the proportion of network bandwidth dedicated to NIDS based on network traffic volume. The mathematical equation for bandwidth allocation B_A is expressed in Eq.(9).

$$B_A = \frac{F \times \eta}{B_{total}} \tag{9}$$

where F is the traffic flow rate, η represents a prioritization factor that scales bandwidth for critical periods, and B_{total} denotes the total available bandwidth. Through dynamic adjustments, NIDS can prioritize its share of bandwidth during high-risk periods, ensuring uninterrupted monitoring and data transmission for intrusion detection purposes.

Energy Consumption Monitoring

To maximize efficiency in resource usage, monitoring energy consumption. E_C provides insights into system sustainability. Energy consumption, directly affected by resource allocation.

$$E_C = P \times W \times T \quad (10)$$

where in Eq.(10), P represents the number of packets processed, W denotes the power requirement per packet in watts, and T stands for the total processing time. Regular monitoring of E_C enables NIDS to identify high-energy consumption scenarios, prompting resource adjustments to maintain energy efficiency without compromising detection quality.

Real-Time Memory Allocation

Real-time memory allocation adjusts memory resources based on incoming packet rates and processing needs. Real-time memory M_R allocation ensures that NIDS can accommodate active processes without delays. This memory allocation is defined as shown in Eq.(11).

$$M_R = \frac{C_L}{M_{total}} \times 100 \quad (11)$$

where C_L denotes the computational load and M_{total} indicates the maximum memory capacity. Monitoring M_R allows NIDS to adapt memory usage dynamically, preventing memory saturation while supporting active threat detection.

Strategic Reallocation Decision Making

Adaptive Resource Allocation in OEND encompasses real-time adjustments and strategic reallocation based on anticipated network demands and threat levels. This structured process supports efficient operation, preparing NIDS to respond flexibly under fluctuating conditions while ensuring optimal use of system resources.

3.3 Signature Library Prioritization in OEND

Signature Library Prioritization focuses on organizing and optimizing the signature database to improve the efficiency of NIDS. Just as orangutans prioritize resources based on their immediate needs and environmental conditions, this phase optimizes the detection process by prioritizing high-risk signatures, ensuring that NIDS swiftly detects and responds to the most significant threats. By analyzing and categorizing signatures according to threat levels and frequency, Signature Library Prioritization enables adaptive, targeted detection that minimizes latency while maximizing security.

Frequency-Based Signature Weight Calculation

In Signature Library Prioritization, high-frequency attack patterns are assigned greater importance to enhance detection accuracy. Calculating the frequency-based weight W_f of a signature helps determine its relevance within the database.

$$W_f = \frac{N_a}{N_t} \quad (12)$$

In Eq.(12), where N_a denotes the number of appearances of a particular signature, and N_t represents the total signatures observed in the network over a specified timeframe. By calculating W_f, this step assigns a priority level to signatures based on their occurrence rates. Higher values of W_f indicate more frequently encountered threats, prioritizing them within the detection system and enabling rapid responses to common attack vectors.

Severity-Based Signature Weight Calculation

To address the impact of different threats, a severity-based weight calculation determines the criticality of each signature. Severity-based weight W_s allows NIDS to allocate more resources to high-impact signatures. The equation for severity-based signature weight W_s is expressed mathematically in Eq.(13).

$$W_s = I \times S \quad (13)$$

where I represents the impact level of the signature, and S denotes its severity score. This calculation assigns priority based on the potential damage associated with each attack pattern, ensuring that signatures related to severe threats receive greater attention. By considering both frequency and severity, Signature Library Prioritization optimizes detection accuracy across various attack types, balancing efficiency and effectiveness.

Combined Signature Priority Score

The combined priority score P_c integrates both frequency and severity metrics, generating a unified priority index for each signature in the library. This approach allows NIDS to prioritize signatures based on a weighted sum, balancing frequency with severity for optimized detection. The equation for calculating the combined signature priority score P_c is expressed mathematically in Eq.(14).

$$P_c = \alpha W_f + \beta W_s \quad (14)$$

where α and β represent weight coefficients assigned to frequency-based and severity-based scores, respectively, the values of α and β reflect the relative importance of frequency and severity in the prioritization strategy, enabling customization based on network requirements. By adjusting α and β, Signature Library Prioritization ensures adaptive, context-sensitive resource allocation that supports the timely detection of critical threats.

Dynamic Signature Ranking

Dynamic Signature Ranking arranges the signature library in descending order of priority, according to the combined priority score calculated for each entry. This ordered structure supports NIDS in evaluating the highest-risk signatures first, expediting the identification of critical threats. A mathematical sorting function can represent the ranking process, where the highest-ranked signatures appear at the top.

$$Rank(S_i) = sort(P_c) \quad (15)$$

In Eq.(15), where S_i indicates a specific signature, and $sort(P_c)$ signatures based on their combined priority scores P_c. This prioritized structure enhances detection speed by focusing computational resources on the most relevant threats, aligning with OEND's adaptive principles. By organizing signatures dynamically, NIDS can adapt to evolving threat landscapes, maintaining a high vigilance against emerging attacks.

Weighted Detection Threshold

Weighted detection thresholds refine the intrusion detection by setting flexible limits for identifying priority signatures. A detection threshold T_d defines the sensitivity level of NIDS, adjusting detection focus based on priority scores. The weighted detection threshold is calculated as shown in Eq.(16).

$$T_d = \gamma \times max(P_c) \quad (16)$$

where γ is a threshold adjustment coefficient and $max(P_c)$ represents the maximum combined priority score in the signature library. By setting T_d, Signature Library Prioritization enables NIDS to distinguish between low-priority patterns and critical threats, balancing accuracy with responsiveness. Adjusting γ according to network conditions aligns NIDS detection with OEND's resource-efficient principles.

Signature Expiry Management

Signature Expiry Management, a crucial prioritization aspect, involves assigning expiry times to signatures based on their relevance and current threat landscape. Signatures nearing obsolescence receive lower priority, preserving computational resources for high-risk or emerging threats. The expiry time E_t for a given signature is defined as expressed mathematically in Eq.(17).

$$E_t = \frac{C_p}{U_r} \quad (17)$$

where C_p denotes the cumulative priority of the signature and U_r represents its usage rate within the recent monitoring period. Expiry management ensures that outdated signatures do not consume resources unnecessarily, aligning NIDS with OEND's adaptive efficiency goals.

3.4 Real-Time Anomaly Detection in OEND

Real-time anomaly Detection in the OEND framework is essential for identifying unexpected deviations in network behaviour as they happen. Inspired by the keen environmental awareness of orangutans, this phase operates dynamically to detect irregularities in network traffic that may indicate potential security threats. Building upon the previous steps, Real-Time Anomaly Detection leverages the optimized Signature Library and Adaptive Resource Allocation to identify anomalies immediately and accurately. Mathematical formulations within this stage enable efficient tracking and processing of network behaviour changes, allowing NIDS to respond promptly to threats.

Anomaly Score Calculation

Calculating an anomaly score A_s provides a numerical measure of deviation in network behaviour, essential for distinguishing regular activity from potential intrusions. The anomaly score A_s can be calculated as shown in Eq.(18)

$$A_s = \frac{|R_c - R_n|}{R_n} \quad (18)$$

where $R_c$represents the current rate of incoming packets and R_n denotes the network's average baseline rate. This calculation establishes a standardized value for detecting changes in traffic rate, helping NIDS identify activity spikes that may

signify a threat. Real-time anomaly Detection uses the anomaly score to prioritize further investigation into unusual patterns.

Threshold-Based Detection Metric

Setting a threshold for detection metrics improves the specificity of anomaly identification. The Threshold T_d for anomaly detection is calculated as represented in Eq.(19).

$$T_d = \mu + k.\sigma \tag{19}$$

where μ is the mean anomaly score based on historical data, σ represents the standard deviation of those scores, and k is a scaling factor determining sensitivity. This threshold allows NIDS to distinguish between routine fluctuations and genuine anomalies, only flagging scores above T_d for further analysis. Adjusting k enhances NIDS adaptability, aligning detection criteria with network conditions.

Cumulative Deviation Analysis

Real-time anomaly Detection incorporates cumulative deviation analysis to assess sustained irregularities in network traffic. The cumulative deviation $D_c$is calculated as represented in Eq.(20).

$$D_c = \sum_{i=1}^{n} (A_s - T_d).I(A_s > T_d) \tag{20}$$

where A_s is the anomaly score, T_d is the detection threshold, and I is an indicator function equal to 1 when $A_s > T_d$ and 0 otherwise. This calculation allows NIDS to assess whether deviations are persistent or momentary, aiding in classifying potential threats. High values of D_c suggest prolonged anomalies, which typically require further investigation.

Z-Score Anomaly Detection

Real-time anomaly Detection uses a Z-score calculation to refine anomaly identification, providing a statistical measure of deviation intensity. The Z-score Z is calculated as represented mathematically in Eq.(21).

$$Z = \frac{A_s - \mu}{\sigma} \tag{21}$$

where A_s denotes the anomaly score, μ is the mean anomaly score, and σ is the standard deviation of anomaly scores. The Z-score quantifies how far a specific score deviates from the average, with higher values signalling significant anomalies. This metric aids in prioritizing severe deviations for immediate action, optimizing NIDS efficiency.

Moving Average Anomaly Detection

A moving average M_a smooths recent anomaly scores, supporting short-term detection of deviations.

$$M_a = \frac{1}{w} \sum_{j=i-w+1}^{i} A_{s_j} \tag{22}$$

In Eq.(22). where w represents the window size and A_{s_j} indicates anomaly scores within the window. The moving average provides a near-real-time trend, enabling rapid detection of abnormal shifts. By adjusting w, NIDS can adapt to immediate network changes, capturing emerging anomalies in real-time.

Cumulative Sum (CUSUM) Analysis

The cumulative sum S offers a continuous anomaly tracking method, valuable for identifying gradual shifts in network behavior.

$$S_i = S_{i-1} + \left(A_{s_i} - T_d\right) \tag{23}$$

where in Eq.(23), $S_i$denotes the cumulative sum at the i-th time step, A_{s_i} is the anomaly score at that time, and T_d represents the detection threshold. CUSUM highlights accumulative deviations, flagging anomalies that develop progressively over time. This approach aligns with orangutan-like adaptability, detecting slow patterns within NIDS efficiently.

Correlation-Based Anomaly Detection

Correlation-based metrics analyze relationships between anomaly indicators, providing multidimensional insights into network behaviour. The correlation coefficient ρ between two anomaly indicators A_{s1} and A_{s2}.

$$\rho = \frac{\sum(A_{s1} - \mu_{s1})(A_{s2} - \mu_{s2})}{\Sigma(A_{s1} - \mu_{s1})^2 \Sigma(A_{s2} - \mu_{s2})^2} \tag{24}$$

In Eq.(24) where μ_{s1} and μ_{s2} represent the means of A_{s1} and A_{s2}, respectively. Correlation-based analysis detects connections between traffic patterns, enhancing anomaly identification through relational tracking. Strong correlations highlight synchronized anomalies, supporting robust real-time monitoring.

Deviation Probability Calculation

Calculating the probability of deviation assists in assessing the likelihood of anomalies, providing a probabilistic approach to detection. The probability of deviation P_d is calculated as shown mathematically in Eq.(25).

$$P_d = 1 - e^{-\lambda A_s} \quad (25)$$

where λ is a rate parameter defining sensitivity to anomaly scores and A_s is the anomaly score. This probability highlights the risk associated with deviations, enabling NIDS to prioritize responses based on likelihood estimates. Higher P_d values suggest significant deviations, triggering prompt action.

3.5 Clustering Suspicious Patterns in OEND

Clustering Suspicious Patterns in the OEND framework is crucial in grouping related anomalies to identify emerging and complex threats. Inspired by orangutans' social adaptability and pattern recognition, this stage organizes unusual network behaviours into clusters, detecting coordinated attacks and uncovering subtle patterns that may go unnoticed individually. This step optimizes the analysis process by leveraging mathematical clustering techniques, supporting NIDS in categorizing, understanding, and responding to unusual traffic patterns efficiently.

Distance Calculation for Pattern Similarity

A fundamental requirement in clustering is the ability to measure similarity between patterns. Distance-based clustering techniques use Euclidean distance d to quantify how similar or dissimilar two patterns are. The Euclidean distance d between two anomaly points A_i and A_j is calculated is represented mathematically in Eq.(26).

$$d(A_i, A_j) = \sqrt{\sum_{k=1}^{n} (A_{ik}, A_{jk})^2} \quad (26)$$

where A_{ik} and A_{jk} represent the k-th attributes of anomaly points A_i and A_j and n is the number of attributes analyzed. By calculating $d(A_i, A_j)$ NIDS can determine how closely two patterns are related, grouping patterns with shorter distances into the same cluster. Lower distance values indicate higher similarity, an essential factor in clustering suspicious activities effectively.

Centroid Calculation for Cluster Formation

Once distances are calculated, cluster centroids provide a central reference point for each group of similar patterns. The centroid C of a cluster containing m points $A_1, A_2, \ldots, A_m$ is calculated as mathematically depicted in Eq.(27).

$$C = \frac{1}{m} \sum_{i=1}^{m} A_i \quad (27)$$

where A_i represents each anomaly pattern within the cluster. The centroid calculation establishes a mean position within each group, allowing new patterns to be compared to this central reference for cluster assignment. As new anomalies emerge, comparing them to cluster centroids aids in dynamically adjusting clusters to maintain relevance.

Intra-Cluster Variance Calculation

Intra-cluster variance V_{intra} measures the spread of patterns within a cluster, capturing how closely related the grouped patterns are. The equation for intra-cluster variance is calculated as represented mathematically in Eq.(28).

$$V_{intra} = \frac{1}{m} \sum_{i=1}^{m} d(A_i, C)^2 \quad (28)$$

where $d(A_i, C)$represents the Euclidean distance between each pattern A_i and the cluster centroid C. Lower variance values indicate tighter clusters, suggesting substantial pattern similarity, while higher values imply diversity within the group. Intra-cluster variance helps identify cohesive patterns, refining the clustering process for precise anomaly identification.

Inter-Cluster Distance Calculation

Inter-cluster distance D_{inter} represents the separation between different clusters, helping identify distinctly different suspicious patterns. The inter-cluster distance between two centroids C_1 and $C_2$is calculated as shown in Eq.(29).

$$D_{inter} = d(C_1, C_2) \quad (29)$$

where $d(C_1, C_2)$ measures the Euclidean distance between the centroids of clusters. High inter-cluster distances suggest that clusters are well-separated, reducing the risk of overlap and enhancing the accuracy of anomaly categorization. This measure supports clustering by ensuring distinct separation between unique anomaly types, mirroring

orangutans' instinct to identify different patterns in their Environment.

Cluster Density Calculation

Cluster density D_c measures how closely packed the patterns are within each cluster, reflecting the anomaly concentration. The density D_c of a cluster with m patterns and a defined radius r is calculated as mathematically represented in Eq.(30).

$$D_c = \frac{m}{\pi r^2} \tag{30}$$

where r denotes the maximum distance from the centroid to any pattern in the cluster, higher density values indicate concentrated anomalies, assisting in recognizing areas with intense suspicious activity. Cluster density aids NIDS in prioritizing high-density areas for deeper analysis, aligning with OEND's efficiency-based clustering strategy.

Silhouette Score Calculation

The silhouette score S evaluates the compactness and separation of each cluster, indicating clustering quality. The silhouette score for a pattern A_i is calculated as represented mathematically in Eq.(31).

$$S(A_i) = \frac{b(A_i) - a(A_i)}{max\big(a(A_i), b(A_i)\big)} \tag{31}$$

where $a(A_i)$ is the average distance between A_i and all other points in its cluster, and $b(A_i)$ represents the average distance between A_i and points in the nearest neighbouring cluster. The silhouette score quantifies clustering accuracy, with higher values indicating well-defined clusters. This measure refines cluster formation, optimizing NIDS precision.

Cluster Validity Index Calculation

The cluster validity index $V_{cluster}$ combines intra-cluster variance and inter-cluster distance to assess cluster quality.

$$V_{cluster} = \frac{V_{intra}}{D_{inter}} \tag{32}$$

In Eq.(32), where V_{intra} is the intra-cluster variance, and D_{inter} is the inter-cluster distance. Lower values indicate well-defined clusters with minimal overlap, enhancing NIDS' capability to distinguish between different anomaly types. This index helps maintain clustering quality, refining suspicious pattern analysis in alignment with OEND's precision objectives.

Density-Based Anomaly Detection

Density-based clustering identifies outliers by comparing local density with global density values. The density anomaly score A_d for a pattern A_i is calculated as represented mathematically in Eq.(33).

$$A_d = \frac{\rho(A_i)}{\rho_{global}} \tag{33}$$

where $\rho(A_i)$ denotes the local density around A_i, and ρ_{global} represents the overall density across clusters. Values greater than 1 suggest an anomaly, marking outliers for further analysis. Density-based scores refine detection by highlighting irregularities within clusters, supporting NIDS in focusing on isolated anomalies. The clustering phase in OEND optimizes anomaly categorization by organizing suspicious patterns into meaningful groups, supporting prompt, precise threat detection. By refining clusters using optimized mathematical techniques, NIDS gains a robust framework for recognizing complex attack patterns and enhancing real-time security responses.

3.6. Behavioral Analysis and Contextual Awareness in OEND

Behavioral Analysis and Contextual Awareness in the OEND framework examine network behavior concerning historical patterns and environmental factors. This phase enables NIDS to differentiate between legitimate fluctuations and genuine threats by evaluating anomalies within their operational context. Modeled on orangutans' instinctive awareness and adaptability to their surroundings, this step incorporates behavior-based monitoring, leveraging contextual information to refine the detection process.

Behavioral Similarity Calculation

Behavioral similarity analysis helps identify recurrent activity patterns, distinguishing between regular and unusual network behaviors. The similarity S between current behavior B_c and baseline behavior B_b is quantified.

$$S = \frac{\sum_{i=1}^{n}(B_{ci} \times B_{bi})}{\sqrt{\sum_{i=1}^{n} B_{ci}^2} \times \sqrt{\sum_{i=1}^{n} B_{bi}^2}} \tag{34}$$

In Eq.(34), where B_{ci} and B_{bi} represent the i-th attributes of current and baseline behaviors, respectively, and n is the total number of attributes analyzed. Similarity values close to 1 indicate high resemblance, while lower values suggest deviations

that warrant further inspection. By focusing on behavioral similarities, NIDS can quickly spot atypical activities, refining the intrusion detection process.

Deviation Intensity Score

Deviation intensity quantifies the extent of behavioral shifts within the network. Calculating deviation intensity, D allows NIDS to assess whether observed behavior warrants further scrutiny. The formula for deviation intensity D is represented mathematically in Eq.(35).

$$D = \sum_{j=1}^{m} |B_{cj} - B_{bj}| \quad (35)$$

where B_{cj} and B_{bj} represent the j-th attributes of current and baseline behaviors, and m is the number of attributes examined. High deviation intensity scores indicate notable behavioral changes, drawing attention to potential threats. Deviation intensity measures enhance contextual awareness by tracking shifts in real-time, aligning with OEND's responsiveness.

Behavioral Trend Slope

The slope of behavioral trends captures patterns within network activity changes, offering a temporal dimension to anomaly detection. Behavioral trend slope T_s is calculated as depicted mathematically in Eq.(36).

$$T_s = \frac{\sum_{k=1}^{p}(t_k - \bar{t})(B_{ck} -)}{\sum_{k=1}^{p}(t_k - \bar{t})^2} \quad (36)$$

where t_k represents the time variable, B_{ck} is the behavior at a time? $t_k, \bar{t}$ is the average time and $\bar{B_c}$ is the average behavior. Trend slope T_s indicates the direction and rate of behavior change, assisting in identifying gradual shifts. NIDS can detect evolving anomalies by monitoring slopes, reinforcing OEND's adaptability.

Temporal Consistency Analysis

Temporal consistency analysis assesses how behaviour aligns with expected time-based patterns, focusing on deviations from regular scheduling. Temporal consistency C_t is calculated as shown in Eq.(37).

$$C_t = \frac{1}{q}\sum_{l=1}^{q} |B_{cl} - B_{bl}| \quad (37)$$

where B_{cl} and B_{bl} represent the behaviour at corresponding time points l, and q denotes the number of time intervals examined. Low consistency values suggest that network activity remains aligned with typical temporal patterns, while high values signal irregular behavior. Temporal consistency tracking aids NIDS in detecting anomalies occurring at unusual times.

Context-Based Deviation Probability

Context-based deviation probability P_d assesses the likelihood of an observed behaviour being anomalous based on contextual parameters is calculated as shown in Eq.(38)

$$P_d = \frac{1}{1 + e^{-(D-\theta)}} \quad (38)$$

where D is the deviation intensity, and θ is a threshold parameter. This probability score highlights the potential for an anomaly based on how behaviour deviates from the norm. Higher P_d values indicate significant anomalies, helping NIDS prioritize responses based on contextual severity.

Anomaly Duration Tracking

Tracking anomaly duration provides insight into how long abnormal behavior persists, indicating potential threat severity. Anomaly duration T_a is calculated as represented mathematically in Eq.(39).

$$T_a = t_{end} - t_{start} \quad (39)$$

where t_{end} is the end time of the anomaly, and t_{start} is the start time. Prolonged anomaly durations highlight persistent deviations, suggesting threats requiring immediate action. Duration tracking enhances NIDS responsiveness by differentiating transient anomalies from sustained behavioral shifts.

Frequency Pattern Analysis

Frequency pattern analysis evaluates the occurrence rates of specific behaviors within the network. The frequency F of a behavior is calculated as mathematically represented in Eq.(40).

$$F = \frac{Count\ of\ specific\ behavior}{Total\ observations} \quad (40)$$

The numerator is the count of a particular behavior observed, and the denominator represents the total observations over the monitoring period. High-frequency values indicate recurring patterns, which signify legitimate trends or repeated attacks. This analysis supports NIDS in identifying unusual frequency shifts, adding a layer of contextual awareness.

Weighted Contextual Score

Weighted contextual scoring combines multiple behavioral factors, offering a comprehensive assessment of network activity. The weighted contextual score S_c is expressed mathematically in Eq.(41).

$$S_c = w_1.S + w_2.D + w_3.T_s + w_4.C_t \quad (41)$$

where $w_1, w_2, w_3,$ and w_4 are weights assigned to similarity S, deviation intensity D, trend slope T_s, and temporal consistency C_t. This combined score provides a holistic measure, allowing NIDS to prioritize suspicious behaviors based on a weighted assessment of contextually relevant metrics. Behavioral Analysis and Contextual Awareness allow OEND to interpret network behaviour holistically, enabling NIDS to evaluate and prioritize anomalies based on real-time context. These advanced measures support proactive security through enhanced environmental understanding, guiding the system in discerning genuine threats within routine activities.

3.6 Dynamic Rule Adjustment in OEND

Dynamic Rule Adjustment within the OEND framework addresses the need for flexible and responsive threat detection by adapting the intrusion detection rules based on changing network conditions. Inspired by orangutans' strategic adaptability, this stage recalibrates rule priorities, thresholds, and conditions in response to observed behaviours, emerging threats, and network traffic patterns. This process enhances the effectiveness of NIDS, ensuring that detection parameters remain aligned with real-time demands. Mathematical formulations within this phase enable NIDS to recalibrate and optimize rule sets, maximizing detection accuracy while minimizing resource usage.

Rule Priority Weight Calculation

Dynamic Rule Adjustment prioritizes rules according to the potential threat level associated with each detection rule. The priority weight W_p for a rule is calculated as represented mathematically in Eq.(42).

$$W_p = \alpha.R_s + \beta.P_d \quad (42)$$

where $R_s$represents the rule severity score, P_d denotes the probability of deviation (indicating how likely an anomaly is to be a genuine threat), and α and β are weight coefficients. By adjusting these priority weights, NIDS focuses more computational resources on high-risk rules, improving detection speed and accuracy for critical threats.

Dynamic Threshold Adjustment

Thresholds set boundaries within which network behavior remains acceptable, triggering alerts only when conditions exceed these limits. Dynamic threshold T_d is calculated as shown mathematically in Eq.(43).

$$T_d = \mu + \gamma.\sigma \quad (43)$$

where μ is the average behaviour metric value, σ is the standard deviation, and γ is the sensitivity coefficient. Adjusting γ enables threshold recalibration based on current network behaviour patterns, ensuring that NIDS can identify genuine threats without generating excessive false alarms.

Rule Activation Frequency

Rule activation frequency F_r monitors how often specific rules are triggered, allowing NIDS to detect patterns of frequent activation that may suggest refined threshold settings or rule modifications. Rule activation frequency F_r is calculated as shown in Eq.(44).

$$F_r = \frac{N_r}{T} \quad (44)$$

where N_r represents the number of times a rule is triggered, and T is the time interval over which the measurement is taken. High values of F_r indicate frequently triggered rules, suggesting either a persistent threat type or a need for threshold adjustment.

Weighted Average Rule Adjustment

A weighted average approach adjusts detection parameters across multiple rules to manage rules dynamically. The weighted average A_w is calculated as represented mathematically in Eq.(45).

$$A_w = \frac{\sum_{j=1}^{k} W_{pj}.T_{dj}}{\sum_{j=1}^{k} W_{pj}} \quad (45)$$

where W_{pj} denotes the priority weight of the j-th rule, T_{dj} represents its threshold, and k is the total number of rules. This weighted average enables a balanced adjustment, distributing focus according to rule relevance.

False Positive Rate Calculation

Dynamic Rule Adjustment relies on minimizing false positives to improve detection reliability. The false positive rate F_p for a rule is calculated as represented mathematically in Eq.(46).

$$F_p = \frac{N_{false}}{N_{total}} \quad (46)$$

where N_{false} represents the number of false positives triggered by the rule and N_{total} is the total activations of the rule. A high false positive rate indicates that the rule requires modification to improve accuracy, reducing unnecessary alerts.

False Negative Rate Monitoring

Monitoring the false negative rate F_n is essential in ensuring that critical threats are not missed. The false negative rate F_n is calculated as shown in Eq.(47).

$$F_n = \frac{N_{missed}}{N_{threat}} \quad (47)$$

where N_{missed} represents the number of missed genuine threats and N_{threat} is the total number of verified threats. High false negative rates suggest that the rule thresholds might be too lenient, requiring adjustment for increased sensitivity.

Adaptive Rule Deactivation

Dynamic Rule Adjustment includes adaptive deactivation to manage rule set complexity. The deactivation threshold D_t is calculated based on rule activity and priority.

$$D_t = W_p \times (1 - F_r) \quad (48)$$

In Eq.(48), where W_p is the priority weight and F_r is the rule activation frequency. Low values of D_t indicate rules that are either low priority or rarely activated, justifying temporary deactivation to conserve resources.

Rule Sensitivity Scaling

Sensitivity scaling adjusts each rule's response to align with network conditions, applying a multiplier. S_s to fine-tune detection sensitivity. Sensitivity scaling S_s is calculated as expressed in Eq.(49).

$$S_s = W_p \times \left(\frac{1}{F_p + 1}\right) \quad (49)$$

where W_p is the rule priority weight, and F_p is the false positive rate. High values of S_s indicate a well-calibrated rule with low false positives, enhancing its relevance within NIDS.

Rule Expansion Factor

The rule expansion factor E_r adjusts the detection scope for each rule, broadening or narrowing criteria as needed. The expansion factor E_r is calculated as shown in Eq.(50).

$$E_r = \frac{1}{F_n + 1} \quad (50)$$

where F_n is the false negative rate. Low false negative rates enable more comprehensive rule application, enhancing rule flexibility without compromising detection accuracy. Through these calculations and strategic adjustments, Dynamic Rule Adjustment enhances NIDS by ensuring rules remain flexible, accurate, and responsive to shifting network demands.

3.7 Automated Response Protocols in OEND

Automated Response Protocols within the OEND framework focus on implementing preemptive actions and rapid reactions to security threats based on real-time detections. Drawing from the strategic responsiveness of orangutans in confronting environmental risks, this phase equips NIDS with immediate response capabilities, enabling the system to isolate threats, mitigate risks, and secure network integrity efficiently. By setting up automated responses that trigger specific actions under predefined conditions, NIDS can maintain a resilient security stance without manual intervention. Mathematical equations within this stage guide decision-making processes, ensuring responses are proportionate, efficient, and adaptive.

Risk Assessment Calculation

The first step in automated response protocols involves calculating a risk assessment score to determine the urgency of response actions. The risk score R_s is calculated as expressed mathematically in Eq.(51).

$$R_s = W_p . P_d \quad (51)$$

where $W_p$represents the priority weight of the rule associated with the detected threat and P_d is the probability of deviation as calculated in previous steps. A high R_s indicates an elevated threat level, signaling the need for an immediate response.

Action Severity Scaling

Once the risk level is calculated, the severity of the response action is scaled to match the threat intensity. Action severity $A_s$is defined as shown in Eq.(52).

$$A_s = R_s \times \delta \tag{52}$$

where R_s is the calculated risk score, and δ is a response coefficient determined by network policy or security requirements. Higher values of A_s correspond to more severe actions, such as blocking access or isolating affected devices.

Response Delay Adjustment

Delays in response can increase vulnerability, making prompt action crucial. The response delay T_r for each action is calculated as mathematically represented in Eq.(53).

$$T_r = \frac{1}{R_s + 1} \tag{53}$$

where R_s is the risk score. A high-risk score results in a low T_r, minimizing delay and enabling rapid action. This adjustment ensures that higher-risk threats receive faster responses, enhancing the effectiveness of automated protocols.

Isolation Radius Calculation

In instances where threat containment is necessary, calculating the isolation radius I_r defines the range within which affected devices are segregated. Isolation radius I_r is determined by Eq.(54).

$$I_r = \frac{A_s}{\eta} \tag{54}$$

where A_s is the action severity, and η is a containment factor that scales the isolation area based on network topology. A higher I_r means a broader isolation area, enabling comprehensive containment of the threat.

Device Quarantine Duration

In cases of device-specific anomalies, quarantine duration Q_d specifies the period during which affected devices remain isolated. The quarantine duration Q_d is calculated as represented mathematically in Eq.(55).

$$Q_d = A_s \times \tau \tag{55}$$

where A_s is the action severity, and τ is a duration factor tailored to network policies. Higher severity actions lead to longer quarantine times, allowing for an extensive evaluation of the affected device's behavior.

Containment Level Adjustment

Automated responses vary based on the containment level required. The containment level C_l is adjusted as represented mathematically in Eq.(56).

$$C_l = \frac{W_p}{F_p + 1} \tag{56}$$

where $W_p$represents the rule priority weight and F_p is the false positive rate of the rule. High containment levels are applied to high-priority rules with low false favorable rates, ensuring that containment efforts are focused on verified threats.

Automated Blocking Probability

Blocking network access is a critical response action in high-risk situations. The automated blocking probability P_b is defined as shown in Eq.(57).

$$P_b = \frac{R_s}{R_s + k} \tag{57}$$

where R_s is the risk score, and κ is a tolerance parameter reflecting acceptable risk thresholds. Higher R_s values yield higher P_b, indicating a greater likelihood of blocking access as a preventive measure.

Recovery Protocol Activation Time

Recovery protocols help restore normalcy following containment actions. The activation time for recovery $T_{recocery}$ is calculated as expressed mathematically in Eq.(58).

$$T_{recovery} = \frac{Q_d}{A_s} \tag{58}$$

where Q_d is the quarantine duration and A_s is the action severity. More extended quarantines paired with lower severity prompt gradual recovery, while higher severity cases initiate faster restoration post-containment.

Alerting Frequency Control

Alerting frequency F_a controls notification intervals to prevent alert fatigue while ensuring real-time threat awareness. The alerting frequency F_a is calculated using the Eq.(59).

$$F_a = \frac{1}{R_s + \lambda} \tag{59}$$

where R_s is the risk score, and λ is an alerting threshold factor. High-risk scores result in frequent alerts, informing security teams of critical situations. Automated Response Protocols within OEND optimize NIDS reaction capabilities through these calculated responses, aligning response actions to the intensity and urgency of detected threats.

3.8 Continuous Learning and Feedback Integration in OEND

Continuous Learning and Feedback Integration, as the final step in OEND framework, strengthens NIDS by enabling adaptive improvement based on ongoing analysis and historical data. This phase emulates orangutans' natural learning and adaptation skills, where past experiences inform future behaviour by integrating feedback to refine detection algorithms and update the threat database continuously. This cyclical process enhances NIDS's accuracy and responsiveness, adjusting detection and response mechanisms to evolving threat landscapes. Mathematical modelling within this step supports adaptive learning, providing a robust foundation for ongoing system optimization.

Error Rate Monitoring

An essential component in feedback integration involves monitoring error rates to evaluate NIDS accuracy. The error rate E is defined as shown in Eq.(60).

$$E = \frac{N_{false} + N_{missed}}{N_{total}} \quad (60)$$

where N_{false} represents the number of false positives, N_{missed} indicates the count of false negatives and N_{total} is the total number of alerts generated. Monitoring E identifies areas requiring refinement, guiding NIDS in improving detection parameters for higher accuracy.

Learning Rate Adjustment

In continuous learning, adjusting the learning rate L_r controls the speed at which detection algorithms incorporate new data. The learning rate is determined by Eq.(61).

$$L_r = \frac{1}{1 + \alpha . T} \quad (61)$$

where α is a decay factor that moderates learning speed, and T represents the time elapsed since the last update. High L_r values enable rapid adaptation, while lower values ensure stability and gradual learning.

Feedback Weight Calculation

Incorporating feedback relies on assigning weights to historical data points to assess their relevance to current behavior. The feedback weight W_f for a specific data point is calculated as represented mathematically in Eq.(62).

$$W_f = e^{-\beta T} \quad (62)$$

where β is a weighting factor, and T denotes the age of the data point. Older data receives lower weights, ensuring that recent patterns have a more significant impact on learning processes.

Anomaly Pattern Update Frequency

The frequency of updates to anomaly patterns maintains NIDS's responsiveness to emerging threats. The anomaly pattern update frequency F_u is calculated as expressed in Eq.(63).

$$F_u = \frac{N_{new}}{T_{update}} \quad (63)$$

where N_{new} represents the number of new anomaly patterns detected and T_{update} is the time interval since the last update. High F_u values indicate rapid learning, adapting detection rules to recent threat trends.

Pattern Matching Accuracy Improvement

Improving pattern-matching accuracy is critical in minimizing false positives and missed detections. Pattern matching accuracy A_m is calculated as expressed mathematically in Eq(64).

$$A_m = \frac{N_{correct}}{N_{total}} \quad (64)$$

where $N_{correct}$ is the count of accurately matched patterns and N_{total} denotes all pattern matches attempted. Monitoring A_m highlights the effectiveness of detection algorithms, supporting NIDS in refining matching criteria.

Weighting of New Anomalies

Weighting newly identified anomalies relative to established patterns supports NIDS in focusing on recent threats. The weight of a new anomaly W_a is calculated as shown in Eq.(65).

$$W_a = \frac{N_{recent}}{N_{total}} \quad (65)$$

where N_{recent}represents the recent anomaly count within a specified timeframe and N_{total} denotes

all detected anomalies. Higher W_a values reflect a greater emphasis on recent behavior, supporting timely adaptation to evolving threats.

Data Retention Period Adjustment

Adjusting the data retention period R_d ensures that NIDS maintains relevant information without overwhelming the system. The retention period R_d is calculated as represented mathematically in Eq.(66).

$$R_d = \frac{C}{D_{usage}} \quad (66)$$

where C represents data capacity and D_{usage} is the rate of data access for learning purposes. A shorter R_d retains only recent data, optimizing system efficiency.

Continuous Anomaly Scoring Update

Updating anomaly scores continuously enhances NIDS sensitivity to new data. The updated anomaly score A'_s is defined as Eq.(67).

$$A'_s = \lambda . A_s + (1 - \lambda) . A_n \quad (67)$$

where A_s is the previous anomaly score, A_n is the new anomaly score, and λ is a weighting factor that balances historical and recent scores. Higher A'_s values indicate significant anomalies, highlighting areas for rule refinement.

Feedback Integration Coefficient

A feedback integration coefficient I_f supports controlled learning based on observed effectiveness. The coefficient I_f is calculated as shown in Eq.(68).

$$I_f = \frac{E_{reduction}}{E_{initial}} \quad (68)$$

where $E_{reduction}$ denotes the decrease in error rate after adjustments and $E_{initial}$ represents the initial error rate before feedback application. High I_f values suggest effective learning, guiding NIDS in incorporating successful patterns. The Continuous Learning and Feedback Integration phase within OEND utilizes these calculated metrics to refine detection accuracy, adapt to new threats, and support proactive security management. This step sustains a dynamic learning process, empowering NIDS to recognize emerging patterns while enhancing resilience through data-driven optimization.

The OEND framework provides a comprehensive, adaptive approach to intrusion detection, mirroring the strategic and resourceful behaviors observed in orangutans. Each of the nine stages within the framework from initial Environment scanning to continuous learning contributes to a robust defense system, addressing the specific challenges associated with dynamic network security. Through techniques such as clustering suspicious patterns, dynamic rule adjustment, and automated response protocols, OEND enhances the capacity of NIDS to monitor, detect, and respond to evolving threats in real-time. By incorporating automated learning and feedback integration, OEND continuously refines its detection parameters and response strategies based on historical and new data. This iterative process strengthens the system's ability to recognize established and emerging threats, creating an adaptable defense that aligns with the unpredictable nature of cyber environments. In doing so, OEND improves detection accuracy and efficiency and reduces the resource demands on security personnel by automating critical responses and prioritizing high-risk alerts. The framework's mathematical models further ensure that adjustments are precise, data-driven, and tailored to specific network conditions, optimizing the balance between sensitivity and specificity in intrusion detection. OEND empowers NIDS with enhanced adaptability, accuracy, and resilience, providing a proactive, responsive solution to modern cybersecurity challenges. OEND sets a new standard for sustainable, intelligent network security through this strategically layered defense.

4. DATASET DESCRIPTION

The Network Intrusion Detection dataset, available at Kaggle, offers a comprehensive resource for evaluating intrusion detection systems. This dataset contains labeled data for training and testing machine learning models to identify network anomalies and potential security breaches. It is divided into a training dataset and a testing dataset, the latter accessible through the Test_data.csv file. The dataset includes a rich set of features that capture various network attributes and traffic behaviors, enabling the detection of both normal and malicious activities.

Features include source and destination IP addresses, protocol types, service types, packet counts, and labels indicating whether the traffic is benign or indicative of specific intrusion types. This granularity supports the analysis of diverse

attack vectors such as denial-of-service (DoS), unauthorized access, and reconnaissance. With 22,544 samples, the dataset is well-suited for building and testing supervised machine learning models. The labeled nature of the data ensures that models can be trained with high accuracy. Its focus on real-world network activity provides practical insights for developing robust NIDS solutions. This dataset serves as a valuable benchmark for advancing intrusion detection research, particularly in dynamic and resource-constrained environments like IoMT.

4.1 Research Method Protocol

The experimental protocol evaluates the proposed Orangutan-Enhanced Network Defense (OEND) framework using a labelled network intrusion detection dataset obtained from Kaggle. The dataset contains 22,544 samples and includes network traffic attributes and corresponding labels for identifying benign and malicious activities. The experimental procedure follows a structured sequence. First, the dataset is examined to identify the available traffic features, class labels, and data distribution. Second, the data are prepared for model evaluation using the preprocessing operations applied in the experiment. Third, the prepared data are supplied to the OEND framework, which organizes the detection process into nine stages: environment scanning, adaptive resource allocation, signature library prioritization, real-time anomaly detection, suspicious-pattern clustering, behavioural analysis and contextual awareness, dynamic rule adjustment, automated response, and continuous learning and feedback integration. Fourth, the performance of OEND is compared with DI-NIDS and DMAN under the experimental configuration used in the study. Finally, classification accuracy, F-measure, precision, recall, attack detection rate, and missed detection rate are used to assess and compare the detection outcomes. The reported results are presented using tables and graphical representations to facilitate comparison across the evaluated approaches. Reproduction of the experiment requires the dataset source and version, exact training and testing partition, preprocessing procedures, implementation environment, model-specific parameter settings, and random seed to be documented alongside the protocol.

5. RESULTS AND DISCUSSIONS

Results and discussion interpret the evaluated outcomes of various metrics to highlight system performance, strengths, and limitations. This section analyzes observed data to compare algorithms' efficiency and identify key insights for improvement. The comparison involves three classification algorithms: DI-NIDS, DMAN, and OEND evaluated using different metrics like Classification Accuracy (CL-AC), F-Measure (F-MSR), Precision (PREC) and Recall (RCLL). Classification Accuracy measures the percentage of correctly identified instances (both normal and malicious) out of the total instances. F-Measure represents the harmonic mean of precision and recall, balancing detection accuracy and error rate. Fig1. Depicts the obtained results of two metrics CL-AC and F-MSR.

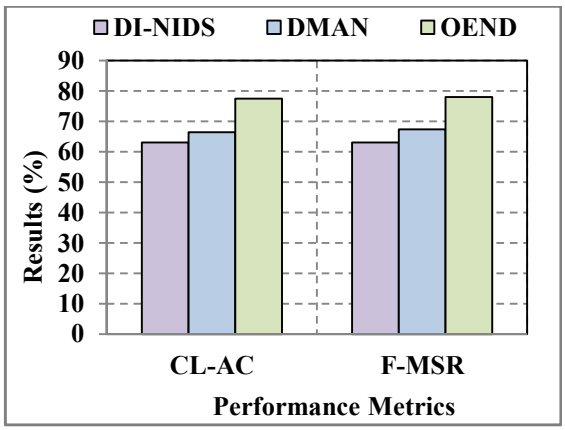


Figure 1: CL-AC and F-MSR

OEND achieves the highest performance, with 77.512% CL-AC and 77.941% F-MSR, demonstrating its superior ability to identify network intrusions with accuracy and efficiency. DMAN records moderate performance, with 66.397% CL-AC and 67.327% F-MSR, indicating improvement over DI-NIDS but limited in precision and recall balance. DI-NIDS achieves the lowest metrics, with 63.090% CL-AC and 63.071% F-MSR, highlighting its reduced capability in complex intrusion detection scenarios. The results emphasize the advanced optimization in OEND, making it a reliable solution for robust intrusion detection in dynamic network environments.

Precision (PREC) evaluates the proportion of correctly identified positive instances among all instances flagged as positive, reflecting the system's ability to avoid false positives. Recall (RCLL) measures the proportion of correctly identified positive instances out of all actual positive instances, representing the system's

sensitivity to identifying true intrusions. Fig 2. Illustrate the obtained results of PREC and RCLL.

OEND demonstrates the highest performance, achieving 79.698% PREC and 76.259% RCLL. This indicates OEND's ability to precisely detect intrusions while maintaining high sensitivity to true positives. DMAN records moderate performance with 66.091% PREC and 68.610% RCLL, showing an improvement in recall but relatively lower precision compared to OEND. DI-NIDS achieves the lowest scores, with 59.285% PREC and 67.373% RCLL, indicating challenges in minimizing false positives and maintaining sensitivity.

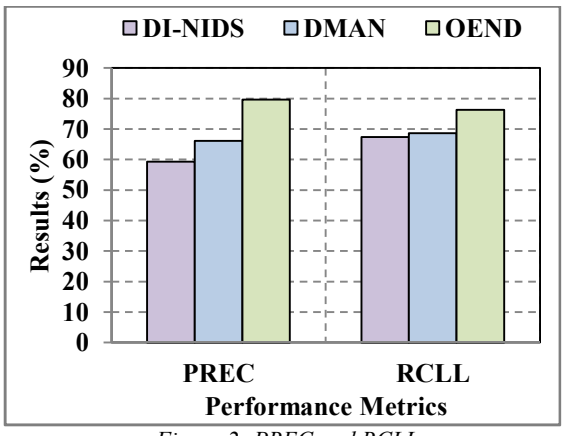


Figure 2: PREC and RCLL

The results highlight OEND's superior optimization in balancing detection precision and recall, making it well-suited for complex network intrusion detection tasks. The improvement over DMAN and DI-NIDS underscores the importance of advanced methodologies in achieving robust and reliable performance in dynamic network environments.

Table 1. ADR, MDR and DR

Classification Algorithms	ADR	MDR	DR
DI-NIDS	67.373	32.627	63.090
DMAN	68.610	31.390	66.397
OEND	76.259	23.741	77.512

The Table 1 presents a performance comparison of three classification algorithms DI-NIDS, DMAN, and OEND evaluated using the metrics Attack Detection Rate (ADR), Missed Detection Rate (MDR), and Detection Rate (DR). Attack Detection Rate (ADR) measures the proportion of attacks correctly identified out of the total attacks, with higher values indicating better detection capabilities. Missed Detection Rate (MDR) represents the proportion of attacks that were undetected, where lower values reflect stronger system performance. Detection Rate (DR) evaluates the overall ability of the system to correctly classify both normal and malicious traffic, combining true positives and true negatives into a single metric.

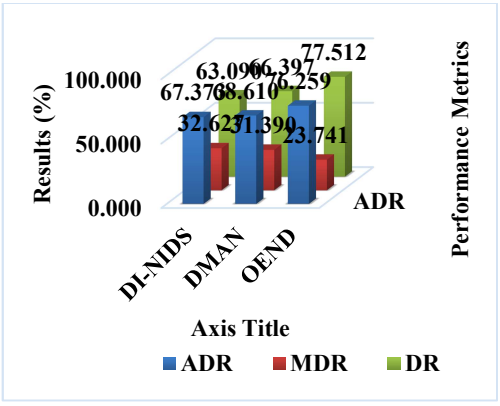


Figure 3: Detection Rates

Fig 3. Illustrates the Otained results in pictorial format, OEND achieves the highest performance with an ADR of 76.259%, MDR of 23.741%, and DR of 77.512%, showcasing its superior ability to detect attacks, minimize missed detections, and accurately analyze network traffic. DMAN performs moderately, recording an ADR of 68.610%, MDR of 31.390%, and DR of 66.397%, indicating improvement over DI-NIDS but limited in overall efficiency compared to OEND. DI-NIDS records the lowest performance, with an ADR of 67.373%, MDR of 32.627%, and DR of 63.090%, highlighting challenges in balancing attack detection and minimizing missed detections. The analysis underscores OEND's effectiveness in optimizing detection capabilities, achieving a robust balance between accuracy and efficiency, and making it the most suitable option for complex and dynamic network intrusion scenarios. DMAN provides moderate improvements, while DI-NIDS reflects baseline performance in intrusion detection tasks.

5.1 Open Issues and Research Limitations

Despite the encouraging comparative results, several open issues remain unresolved in the present study. The evaluation uses a network intrusion detection dataset containing 22,544 samples, and the reported findings do not establish generalizability to real-world 6G-enabled Internet of Medical Things (IoMT) environments. Performance under encrypted traffic, previously

unseen attacks, changing healthcare communication patterns, and heterogeneous medical devices remains to be investigated. The study also does not establish the computational overhead, processing latency, memory consumption, scalability, or energy requirements of the proposed OEND framework under resource-constrained conditions. The individual contribution of the nine integrated stages has not been isolated through ablation experiments, and the reported comparisons have not been supported by statistical significance testing across repeated independent trials. Further investigation is required to assess false alarm behaviour, resilience against adversarial manipulation, and the practical reliability of automated responses in safety-critical healthcare networks. Future research should address these limitations through reproducible experimental protocols, statistical validation, component-wise evaluation, and testing with healthcare-specific datasets and representative 6G-enabled IoMT traffic. Addressing these open issues would provide stronger evidence of OEND's robustness, efficiency, and suitability for practical deployment.

6. CONCLUSION

The proposed Orangutan-Enhanced Network Defense (OEND) framework addresses the identified research gap by integrating nine interconnected stages encompassing environment scanning, adaptive resource allocation, signature library prioritization, real-time anomaly detection, suspicious-pattern clustering, behavioural analysis and contextual awareness, dynamic rule adjustment, automated response, and continuous learning and feedback integration. Unlike approaches that focus on individual aspects of intrusion detection, OEND combines detection, adaptation, and response mechanisms within a unified framework. Comparative evaluation against DI-NIDS and DMAN on the selected network intrusion detection dataset yielded a classification accuracy of 77.512%, an F-measure of 77.941%, precision of 79.698%, recall of 76.259%, an attack detection rate of 76.259%, and a missed detection rate of 23.741%. The findings address the study's research questions concerning comparative classification performance and attack detection, demonstrating improved reported results over the selected baseline approaches on the evaluated dataset. The principal scientific contribution lies in the coordinated integration of adaptive detection and response stages rather than in any individual technique alone. Nevertheless, the findings do not establish statistical significance, the independent contribution of each stage, or validated performance in actual 6G-enabled Internet of Medical Things (IoMT) deployments. Future research should incorporate reproducible implementation details, repeated experimental trials with appropriate statistical tests, ablation studies, and evaluation using healthcare-specific traffic, encrypted communications, previously unseen attacks, and representative 6G-enabled IoMT environments to establish the framework's generalizability, computational efficiency, and practical applicability.

REFERENCES:

[1] R. Karthikeyan and R. Vadivel, “Boosted Mutated Corona Virus Optimization Routing Protocol (BMCVORP) for Reliable Data Transmission with Efficient Energy Utilization,” Wirel Pers Commun, 2024, doi: 10.1007/s11277-024-11155-7.

[2] P. K. Singh and A. Sharma, “An intelligent WSN-UAV-based IoT framework for precision agriculture application,” Computers and Electrical Engineering, vol. 100, p. 107912, 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.107912.

[3] R. Ramya and Dr. T. Brindha, “A Comprehensive Review on Optimal Cluster Head Selection in WSN-IoT,” Advances in Engineering Software, vol. 171, p. 103170, 2022, doi: https://doi.org/10.1016/j.advengsoft.2022.103170.

[4] S. Rani, A. Kataria, S. Kumar, and P. Tiwari, “Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review,” Knowl Based Syst, p. 110658, 2023, doi: https://doi.org/10.1016/j.knosys.2023.110658.

[5] S. Singh, A. S. Nandan, G. Sikka, A. Malik, and A. Vidyarthi, “A secure energy-efficient routing protocol for disease data transmission using IoMT,” Computers and Electrical Engineering, vol. 101, p. 108113, 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.108113.

[6] S. T. Banafshehvaragh and A. M. Rahmani, “Intrusion, anomaly, and attack detection in smart vehicles,” Microprocess Microsyst, vol. 96, p. 104726, 2023, doi: https://doi.org/10.1016/j.micpro.2022.104726.

[7] M. V. B. M. K. M, C. A. Ananth, and N. Krishnaraj, “Detection of intrusions in

clustered vehicle networks using invasive weed optimization using a deep wavelet neural networks," Measurement: Sensors, p. 100807, 2023, doi: https://doi.org/10.1016/j.measen.2023.100807.

[8] B. Madhu, M. Venu Gopala Chari, R. Vankdothu, A. K. Silivery, and V. Aerranagula, "Intrusion detection models for IOT networks via deep learning approaches," Measurement: Sensors, vol. 25, p. 100641, 2023, doi: https://doi.org/10.1016/j.measen.2022.100641.

[9] R. Harini, N. Maheswari, S. Ganapathy, and M. Sivagami, "An effective technique for detecting minority attacks in NIDS using deep learning and sampling approach," Alexandria Engineering Journal, vol. 78, pp. 469–482, 2023, doi: https://doi.org/10.1016/j.aej.2023.07.063.

[10] A. S. Alqahtani, "Deep Convolutional Neural Network for Active Intrusion Detection and Protect data from Passive Intrusion by Pascal Triangle," Wirel Pers Commun, 2024, doi: 10.1007/s11277-023-10846-x.

[11] H. Bangui, M. Ge, and B. Buhnova, "A Hybrid Data-driven Model for Intrusion Detection in VANET," Procedia Comput Sci, vol. 184, pp. 516–523, 2021, doi: https://doi.org/10.1016/j.procs.2021.03.065.

[12] G. F. E and S. Sheeja, "A Novel RDAE Based PSR-QKD Framework for Energy Efficient Intrusion Detection," in 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), 2022, pp. 1–6. doi: 10.1109/ICKECS56523.2022.10060298.

[13] M. Ge, N. F. Syed, X. Fu, Z. Baig, and A. Robles-Kelly, "Towards a deep learning-driven intrusion detection approach for Internet of Things," Computer Networks, vol. 186, p. 107784, 2021, doi: https://doi.org/10.1016/j.comnet.2020.107784.

[14] M. Lima, R. Lima, F. Lins, and M. Bonfim, "Beholder – A CEP-based intrusion detection and prevention systems for IoT environments," Comput Secur, vol. 120, p. 102824, 2022, doi: https://doi.org/10.1016/j.cose.2022.102824.

[15] J. L. Webber et al., "An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks," Computers and Electrical Engineering, vol. 111, p. 108964, 2023, doi: https://doi.org/10.1016/j.compeleceng.2023.108964.

[16] R. Kumar, A. Malik, and V. Ranga, "An intellectual intrusion detection system using Hybrid Hunger Games Search and Remora Optimization Algorithm for IoT wireless networks," Knowl Based Syst, vol. 256, p. 109762, 2022, doi: https://doi.org/10.1016/j.knosys.2022.109762.

[17] P. Srividya and L. N. Devi, "An optimal cluster & trusted path for routing formation and classification of intrusion using the machine learning classification approach in WSN," Global Transitions Proceedings, vol. 3, no. 1, pp. 317–325, 2022, doi: https://doi.org/10.1016/j.gltp.2022.03.018.

[18] A. Nazari, M. Kordabadi, R. Mohammadi, and C. Lal, "EQRSRL: an energy-aware and QoS-based routing schema using reinforcement learning in IoMT," Wireless Networks, 2023, doi: 10.1007/s11276-023-03367-9.

[19] A. Ali et al., "An optimized multilayer perceptron-based network intrusion detection using Gray Wolf Optimization," Computers and Electrical Engineering, vol. 120, p. 109838, 2024, doi: https://doi.org/10.1016/j.compeleceng.2024.109838.

[20] H. Chen, Z. Wang, S. Yang, X. Luo, D. He, and S. Chan, "Intrusion detection using synaptic intelligent convolutional neural networks for dynamic Internet of Things environments," Alexandria Engineering Journal, vol. 111, pp. 78–91, 2025, doi: https://doi.org/10.1016/j.aej.2024.10.014.

[21] M. A. Alkhonaini et al., "Sandpiper optimization with hybrid deep learning model for blockchain-assisted intrusion detection in iot environment," Alexandria Engineering Journal, vol. 112, pp. 49–62, 2025, doi: https://doi.org/10.1016/j.aej.2024.10.032.

[22] Y.-S. Kil, Y.-R. Jeon, S.-J. Lee, and I.-G. Lee, "Multi-Binary Classifiers Using Optimal Feature Selection for Memory-Saving Intrusion Detection Systems," CMES - Computer Modeling in Engineering and Sciences, vol. 141, no. 2, pp. 1473–1493, 2024, doi: https://doi.org/10.32604/cmes.2024.052637.

[23] M. Shoab and L. Alsbatin, "GRU Enabled Intrusion Detection System for IoT Environment with Swarm Optimization and Gaussian Random Forest Classification," Computers, Materials and Continua, vol. 81, no. 1, pp. 625–642, 2024, doi: https://doi.org/10.32604/cmc.2024.053721.

[24] T. Kim and W. Pak, "Early Detection of Network Intrusions Using a GAN-Based One-Class Classifier," IEEE Access, vol. 10, pp. 119357–119367, 2022, doi: 10.1109/ACCESS.2022.3221400.

[25] K. He, W. Zhang, X. Zong, and L. Lian, "Network Intrusion Detection Based on Feature Image and Deformable Vision Transformer Classification," IEEE Access, vol. 12, pp. 44335–44350, 2024, doi: 10.1109/ACCESS.2024.3376434.

[26] X. Gao, Q. Wu, J. Cai, and Q. Li, "A Fusional Intrusion Detection Method Based on the Hierarchical Filtering and Progressive Detection Model," IEEE Access, vol. 11, pp. 131409–131417, 2023, doi: 10.1109/ACCESS.2023.3335669.

[27] W. Dai, X. Li, W. Ji, and S. He, "Network Intrusion Detection Method Based on CNN-BiLSTM-Attention Model," IEEE Access, vol. 12, pp. 53099–53111, 2024, doi: 10.1109/ACCESS.2024.3384528.

[28] S. Layeghy, M. Baktashmotlagh, and M. Portmann, "DI-NIDS: Domain invariant network intrusion detection system," Knowl Based Syst, vol. 273, p. 110626, 2023, doi: https://doi.org/10.1016/j.knosys.2023.110626

[29] J. Ramkumar, R. Karthikeyan, and S. P. Priyadharshini, "Temporal GraphSAGE–Based Trust Framework Using Internet Protocol Flow Information Export (TGS-IPFIX) for Scalable Digital Identity Systems in Finternet," International Journal of Computer Networks and Applications, vol. 13, no. 3, pp. 548–567, 2026.

[30] J. Ramkumar, S. Rajagopal, B. Suchitra, and S. Balamurugan, "Graph Neural Networks: Concepts and Applications", Wiley, pp. 1–912, 2026.

[31] C. Balakrishnan, J. Ramkumar, and R. Karthikeyan, "Emotion Journey-Aware VADER (EJ-VADER) Approach for Optimized Sentiment Interpretation in Consumer Behaviour Studies," International Journal of Engineering Trends and Technology, vol. 74, no. 6, pp. 328–342, 2026.

[32] B. Suchitra, J. Ramkumar, and M. M. M. Jawarneh, "Future Trends in Distributed Systems for Metaverse Applications," in Distributed Algorithms and Protocols for the Metaverse, pp. 103–137, 2026.

[33] D. R. Medhunhashini, B. Varun, J. Ramkumar, et al., "Grey Wolf Optimization Enhanced Random Forest Framework for LLM Software Defect Prediction," in Proceedings of the IEEE International Conference on Current Trends in Advanced Computing: Where Technology Meets Expectations (ICCTAC), 2026.

[34] J. Ramkumar, V. Valarmathi, and R. Karthikeyan, "Innovative Sustainable Energy Solutions in Smart Cities: Transforming Urban Landscapes for a Greener Future," in Green Energy and Technology, Part F2003, pp. 333–362, 2026.

[35] R. Karthikeyan, J. Ramkumar, S. P. Priyadharshini, and B. Narasimhan, "Optimized Self-adaptive Intrusion Detection System (SPIDS) for Enhanced Network Security," in Communications in Computer and Information Science, vol. 2822, pp. 71–86, 2026.

[36] J. Ramkumar, B. Narasimhan, S. P. Priyadharshini, and R. Karthikeyan, "Optimizing Intrusion Detection with Bayesian Optimization in Reactive Intrusion Detection Systems (BO-RIDS) for Enhanced Security Performance," in Communications in Computer and Information Science, vol. 2822, pp. 87–104, 2026.

[37] V. Valarmathi, J. Ramkumar, and R. Karthikeyan, "Sustainable 6G Connectivity through Artificial Intelligence Powered Energy Efficiency," in Signal Processing Roadmap: Technologies, Applications, and Future Directions, pp. 29–42, 2026.

[38] J. Ramkumar and V. Valarmathi, "Advanced Real-Time Signal Processing Techniques for Adaptive Beamforming in Beyond 5G Wireless Networks," in Signal Processing Roadmap: Technologies, Applications, and Future Directions, pp. 123–137, 2026.

[39] R. Suganthi, J. Ramkumar, C. K. K. Reddy, et al., "Real-Time Applications of 6G in Augmented Reality/Virtual Reality (AR/VR) Ecosystems," in Landscaping 6G: Unlocking the Power of Ultra-Fast Communication, pp. 175–186, 2026.

[40] J. Ramkumar and S. Vetrivel, "Deep Learning Insights into Defending Against Adversarial Attacks in IoT Systems," in Strategic Approaches to Intrusion Detection in Cloud-IoT Ecosystem, pp. 227–250, 2026.

[41] B. Suchitra, J. Ramkumar, and V. Valarmathi, "Rejuvenated Particle Swarm Optimization-Based Classifier for Big Sentiment Data Classification," in Communications in Computer and Information Science, vol. 2819, pp. 41–54, 2026.

[42] V. Valarmathi, J. Ramkumar, and B. Suchitra, "Classification of Cross-Domain Sentiments in

Big Data Using Renewed Genetic Algorithm," in Communications in Computer and Information Science, vol. 2819, pp. 25–40, 2026.

[43] M. P. Swapna, D. Rajeev, J. Ramkumar, and S. Chandran, "Unveiling Cybercrime Patterns in Kerala: A Machine Learning Approach," in Lecture Notes in Networks and Systems, vol. 1445, pp. 111–122, 2026.

[44] S. P. Priyadharshini, F. Nirmala Irudayam, and J. Ramkumar, "Stable Plithogenic Cubic Sets," Journal of Fuzzy Extension and Applications, vol. 6, no. 2, pp. 410–423, 2025.

[45] B. Suchitra, R. Karthikeyan, J. Ramkumar, and V. Valarmathi, "Enhancing Recurrent Neural Network Performance for Latent Autoimmune Diabetes Detection (LADA) Using Exocoetidae Optimization," Journal of Theoretical and Applied Information Technology, vol. 103, no. 5, pp. 1645–1667, 2025.

[46] J. Ramkumar and D. Ravindran, "Machine Learning and Robotics in Urban Traffic Flow Optimization with Graph Neural Networks and Reinforcement Learning," in Machine Learning and Robotics in Urban Planning and Management, pp. 83–104, 2025.

[47] S. P. Priyadharshini and J. Ramkumar, "Mappings of Plithogenic Cubic Sets," Neutrosophic Sets and Systems, vol. 79, pp. 669–685, 2025.

[48] J. Ramkumar, B. Varun, V. Valarmathi, D. R. Medhunhashini, and R. Karthikeyan, "Jaguar-Based Routing Protocol (JRP) for Improved Reliability and Reduced Packet Loss in Drone Ad-Hoc Networks (DANET)," Journal of Theoretical and Applied Information Technology, vol. 103, no. 2, pp. 696–713, 2025.

[49] S. Suchitra, J. Ramkumar, and R. Karthikeyan, "Frog Leap Inspired Optimization-Based Extreme Learning Machine for Accurate Classification of Latent Autoimmune Diabetes in Adults (LADA)," Journal of Theoretical and Applied Information Technology, vol. 103, no. 2, pp. 472–494, 2025.

[50] J. Ramkumar, V. Valarmathi, and R. Karthikeyan, "Optimizing Quality of Service and Energy Efficiency in Hazardous Drone Ad-Hoc Networks (DANET) Using Kingfisher Routing Protocol (KRP)," International Journal of Engineering Trends and Technology, vol. 73, no. 1, pp. 410–430, 2025.

[51] J. Ramkumar, R. Karthikeyan, and M. Lingaraj, "Optimizing IoT-Based Quantum Wireless Sensor Networks Using NM-TEEN Fusion of Energy Efficiency and Systematic Governance," in Lecture Notes in Electrical Engineering, vol. 1246, pp. 141–153, 2025.

[52] M. P. Swapna, J. Ramkumar, and R. Karthikeyan, "Energy-Aware Reliable Routing with Blockchain Security for Heterogeneous Wireless Sensor Networks," in Lecture Notes in Networks and Systems, vol. 1075, pp. 713–723, 2025.

[53] J. Ramkumar, S. P. Priyadharshini, and B. Pattanaik, "Securing the Skies: Safety Queuing Models for Quantum Drone Ad Hoc Networks," in Mathematical Methods in the Digital Age, vol. 3, pp. 39–53, 2025.

[54] M. P. Swapna, D. Rajeev, J. Ramkumar, and S. Chandran, "Gender Dynamics of Cyber Security Awareness in Kerala, India: Statistical and Machine Learning Approach," in Proceedings of the 2025 Gender and Technology Conference (GTC 2025), 2025.

[55] Ramkumar, J.Mehta, Shilpa, Krishan, Ram, "Bio-Inspired intelligence for smart decision-making", Bio-Inspired Intelligence for Smart Decision-Making,

[56] J. Ramkumar and V. Valarmathi, "Harnessing AI-Driven Models for Sustainable Development in Business Management," in World Sustainability Series, Part F775, pp. 217–238, 2025.

[57] J. Ramkumar, R. Karthikeyan, and S. P. Priyadharshini, "Peregrine Falcon Optimization Routing Protocol (PFORP) for Achieving Ultra-Low Latency and Boosted Efficiency in 6G Drone Ad-Hoc Networks (DANET)," International Journal of Computing and Digital Systems, vol. 17, no. 1, pp. 1–18, 2025.

[58] S. P. Priyadharshini, F. Nirmala Irudayam, and J. Ramkumar, "An Unique Overture of Plithogenic Cubic Overset, Underset and Offset," in Studies in Fuzziness and Soft Computing, vol. 435, pp. 139–156, 2025.

[59] J. Ramkumar, R. Karthikeyan, and V. Valarmathi, "Alpine Swift Routing Protocol (ASRP) for Strategic Adaptive Connectivity Enhancement and Boosted Quality of Service in Drone Ad Hoc Network (DANET)," International Journal of Computer Networks and Applications, vol. 11, no. 5, pp. 726–748, 2024.