Artificial Intelligence System for Tackling Cyber Security Threats Using SD-WAN Software Simulations

Akinya Tokunbo Ojo[1], Osaremwinda Omorogiuwa[2]

[1,2]Department of Computer Science & Information Technology, Igbinedion University Okada, Edo State, Nigeria

Abstract- In today's increasingly connected digital landscape, the threat of cyber attacks is ever present and evolving, posing significant risks to organizational networks and data security. Traditional network security measures, while essential, are often insufficient to counter sophisticated and rapidly changing attack vectors. This inadequacy highlights the need for more advanced and adaptive cyber security systems, such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), which can proactively identify and respond to suspicious activities in real time. However, the effectiveness of IDS/IPS systems is often challenged by several critical issues. This study designs and implements a cyber security system that simulates the functions of an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) in a Software Defined Wide Area Network (SD-WAN) using MATLAB. The primary objective is to identify and respond to suspicious activities within a network by analysing traffic patterns, detecting anomalies, and automatically responding to potential threats. This encompasses the use of operational cyber security strategies, tactics, and processes designed to protect the confidentiality, integrity, and availability of data within an organization's operational environment. The system performance was evaluated based on Precision, Recall, and F1-Score performance metrics indices. The Precision value was calculated as 1.0, which indicates that all instances identified as malicious were indeed malicious. This high precision rate is crucial for minimizing false positives, ensuring that legitimate network activities are not mistakenly flagged as threats. The Recall score was 0.9750, which suggests that the system successfully detected almost all of the malicious activities. The F1-Score, which is the harmonic mean of Precision and Recall, was 0.9873 in this study. The high F1-Score reflects a balanced performance between Precision and Recall, indicating that the system is both accurate and comprehensive in detecting threats. The simulation results demonstrate that the cyber security system designed in this study is highly effective in detecting and responding to malicious activities within a network. With a Precision of 1.0, Recall of 0.9750, and an F1-Score of 0.9873, the system ensures minimal false positives and a near-complete identification of all potential threats. The graphical analysis further supports these findings by providing a clear visual representation of how the system handles normal and malicious traffic. The system's ability to quickly and accurately detect threats, coupled with automated responses, can reduce the risk of successful cyber attacks and protect sensitive data and infrastructure. These results indicate that this study can be applied to various real-world scenarios, making them highly valuable for organizations looking to bolster their cyber-security defenses.

Keywords: Cyber Security Threats, Cyber Attacks, Artificial Intelligence, SD-WAN, MATLAB, Software Simulations

1.INTRODUCTION

The growing use of artificial intelligence in the twenty-first century is influencing a societal and economic shift toward increased automation, data-driven decision-making, and the integration of AI systems into various economic sectors and areas of life, with implications for job markets, healthcare, government, industry, education, propaganda, and disinformation. This raises concerns about the long-term impacts, ethical implications, and hazards of AI, sparking debate about governmental regulations to assure the technology's safety and benefits. The numerous subfields of AI study are organized around specific aims and the usage of certain techniques. AI research has traditionally focused on reasoning, knowledge representation, planning, learning, natural language processing, vision, and robotics assistance. One of the field's long-term goals is general intelligence, or the capacity to execute any work that a person can perform on an equivalent level.

This study involves understanding how Artificial Intelligence (AI) is going to be applied and its usage in cyber security functions using Software Defined Wide Area Network (SD-WAN) software simulations. The goal of Artificial Intelligence (AI) is to create and identify intelligent objects. Workers or users of AI can apply their knowledge to any industry they see fit, so in this sense, AI is a broad field (Markopoulou & Papakonstantinou, 2021). Essentially, AI is what happens when a machine begins to mimic human intelligence and begin self-learning, leading to previously undiscovered solutions something that was previously impossible for a machine. However, algorithmic modelling has made this possible, and AI has become a global term and function. Additionally, AI technologies like expert systems, machine learning, deep learning or neural networks, artificial immune systems, intelligent agents, etc. are being used in a variety of industries, including but not limited to the healthcare, automotive, banking, and insurance sectors.

Moreover, a significant issue facing organizations nowadays is their ability to prevent potential abnormalities. Because of the diversity and likelihood of these unexplained breakouts, companies must prioritize how they defend themselves against these kinds of assaults. To lower the danger of an attack, each organization must thereby identify the types of assaults against which they are most vulnerable (Adewale & Segun, 2024). The uncertainty in the organization has skyrocketed as a result of the current surge in cyberattacks. Agagu et al., (2024) proposes a hybrid ensemble-based machine-learning technique for predicting phishing websites from URLs to address cyber attacks. The research employs three base classifiers: CatBoost, XGBoost, and LightGBM. The voting technique was used to combine the base classifiers to build an ensemble model to help detect phishing websites.

Automation by itself won't be adequate since cyberattacks on the networks of global corporations, including governments, have kept cyber attack prevention teams incredibly busy. However, given the advancement of AI capabilities and techniques, such as machine learning, neural networks or deep learning, expert systems, artificial immune systems, and intelligent agents, there is an increasing need to handle these cyberattacks proactively and with the ability to predict and resolve them. These cutting-edge technologies are revolutionizing cyber security management in modern organizations, which are more susceptible than ever to unknown or unpredictable attacks. The shift is perceived as involving not only managing these cyberattacks proactively but also anticipating and resolving issues before they negatively impact a company's operations and jeopardize the data of its customers (Maglaras, 2021).

Various types of cyber risks, such as ransomware, phishing, data leakage, hacking, Trojan horse, computer worm, DOS and DDOS attacks, adware, and spyware, were typically managed reactively according to traditional practices, which included incident detection and appropriate response to protect the company's network. However, with more sophisticated network assaults, there is an urgent need to manage cyber risks proactively by forecasting and safeguarding businesses with AI technologies. One of the major problems with existing IDS/IPS systems is their tendency to generate a high number of false positives. This not only overwhelms network administrators but also reduces the system's overall efficiency. A high precision score is crucial to ensuring that the IDS/IPS accurately identifies true threats without raising unnecessary alarms. The simulation outputs a high precision score, indicating the system's effectiveness in minimizing false alerts, which is vital for operational efficiency. Another significant problem is the potential for IDS/IPS systems to miss certain types of attacks, leading to incomplete threat detection. A high recall score is essential for ensuring that the system can detect and respond to as many malicious activities as possible. The simulation results, with a high recall score, indicate the system's capability to detect the majority of malicious traffic, thereby addressing the problem of incomplete threat detection.

The challenge of balancing Precision and Recall, often quantified by the F1-Score, is a critical issue in IDS/IPS systems. Achieving high Precision without compromising Recall, and vice versa, is difficult yet essential for an effective security system. The F1-Score generated in the simulation reflects this balance, demonstrating the system's overall robustness in both identifying genuine threats and minimizing false positives.

Traditional IDS/IPS systems often struggle with effectively detecting anomalies and responding in a timely manner. The system's performance in anomaly detection, as shown by the graphs of anomaly scores and detection & response time, is crucial for preventing breaches. The ability to quickly detect and respond to threats, as indicated by the generated graphs, is vital for minimizing the potential damage caused by cyber-attacks. Distinguishing between normal and malicious traffic, and adjusting the system's response accordingly, is another critical problem for IDS/IPS systems. The generated graphs of normal vs. malicious traffic responses and threshold settings highlight the system's capability to adapt to different types of traffic and fine-tune its sensitivity to threats, addressing the problem of incorrect traffic differentiation.

2. LITERATURE REVIEW

The proliferation of technical solutions in various domains such as living, services, machines, and businesses has led to a corresponding rise in cyber attacks and cybercrime. In 2022, 15 billion records (data structures) were exploited, a significant rise from the paltry 103 million exposed records in 2013 (Risk Based Security, 2023). Even advanced intrusion and detection systems may be circumvented by criminals and other attackers nowadays and there are a huge number of exploitations to which individuals and businesses are vulnerable. We can see from the recent past and the COVID-19 outbreak that cybercriminals take advantage of uncertain times. Reed Smits's data (Smith, 2020) indicate a 400% rise in email and internet frauds.

Geographically remote connections that reveal a weak link in the chain at least in one location are one of the several cyber security concerns that exist today. Furthermore, rather of using a proactive recovery approach, computer systems still frequently employ a reactive one (Adewale & Segun, 2024). Reactive approaches are insufficient over the long term and do not guarantee that the same issue will not recur. The estimated costs of cybercrime on a worldwide scale also indicate some concerning tendencies. McAfee's 2023 study states that over $1 trillion has been lost globally as a result of cybercrime (Adewale & Segun, 2024). Many scholars have discussed cyber threats to critical infrastructures and proactive plans to implement comprehensive tactics that include threat detection, prevention, and response. For example, Markopoulou & Papakonstantinou (2021) argued that the idea of "critical infrastructure" is constantly changing to address new issues and take into account current concerns, especially regarding (cyber) security and resilience. As a result, protecting critical infrastructures from various risks has emerged as a key issue globally. Adewale & Segun (2024) argue that as critical infrastructure becomes more digitalized and connected, robust cybersecurity solutions are more important than ever to protect critical systems. According to Roshanaei (2021), a country's infrastructure plays a critical role in determining its ability to grow, innovate, and succeed economically. Durable, well-maintained infrastructure is essential for public safety, health, prosperity, education, and disaster preparedness purposes. Al-Khudaibi et al., (2023) predict potential attacks and threats against critical infrastructure systems by considering attacker intent and applying machine learning models. Using this method, a novel cybersecurity prediction strategy was developed that predicts potential attack strategies based on targets and key infrastructure. The false positive rate (FPR) accuracy of the proposed model using the training and testing datasets was 66%. This proactive approach triples the learned dataset, improving the accuracy of the proposed model in the future to predict potential attack vectors based on specific attacker targets and key infrastructure. According to Rajendran & Vyas (2023), in the past ten years, cyber risks have grown more difficult for experts to handle. More development is required for current security systems to handle highly skilled crooks. Artificial intelligence (AI) tools can be used to detect frauds; however there may be additional hazards involved. As a result, the study's main focus is on the relationship between artificial intelligence (AI) technology and cyber security concerns. Traditional cybersecurity techniques are no longer enough for identifying and thwarting urgent threats. Technological advancements in cryptography and Artificial Intelligence (AI) particularly machine learning have the potential to empower cybersecurity experts to combat the dynamic threat landscape that attackers portray. Rafy (2024) contended that the incorporation of Artificial Intelligence (AI) has had a major impact on the unparalleled speed of technological advancement. AI is pervasive across many industries and has drawn praise and condemnation in equal measure. As it becomes a common element in the creation and operation stages of modern technologies, its expanding application offers both benefits and problems in cybersecurity. Marchal et al., (2024) asserted that Artificial Intelligence (AI) has been used by the cybersecurity industry for more than 20 years, and that it has been applied in a variety of domains, including spam filtering, malware detection, and intrusion detection, in order to improve performance through automation, speed, scalability, and adaptability. Although artificial intelligence has mostly influenced reactive cybersecurity measures, emerging AI technologies show promise for proactive security initiatives such as enhanced security awareness, security risk management, and advanced threat intelligence. However, there are several obstacles in the way of effectively utilizing AI for cybersecurity, and many failed attempts have been made before a viable application was created. According to Chakraborty et al., (2023), technological advancements have led to the automation of every daily work with the arrival of the digital era. According to Ramasubramanian et al., (2021), the advancement of technology poses security issues. Experts require a great deal of assistance in order to prevent security breaches and cyber attacks because connections between organizations result in "Heavy traffic," "Breaches in Security," and "Increase in Security attack vectors," all of which are difficult for people to manage. Developing software with auto-updating logic using technology is a difficult challenge. Katiyar et al., (2024) contended that as cyber-attacks change and become more sophisticated, existing security methods are no longer adequate to secure networks and critical information. Artificial intelligence (AI) and machine learning (ML) approaches provide significant tools for improving cyber security by enabling more effective and efficient threat identification and response. According to Azeez & Chinyere (2024), cyber security is the defense of computational devices and computer networks against information leaks, theft, and damage to their electronic data, software, hardware, or other components, as well as interruption or misrepresentation of the services they provide. Basnet (2022) argued that the emergence of cyber threats has outstripped the cyber defense firm's budgetary capital and human analysis and confronted every new type of cyber danger. With the growing digital footprint, a substantial number of personal info should be safeguarded against cyber attacks. Data breaches can damage a brand’s productivity or cause it to fail. This study investigates the use of artificial intelligence (AI) to improve information security. Chung-hee et al., (2019) investigated raw data from intrusion prevention systems (IPS) and firewalls (FW) with respect to the cyber-attacks against a Korean energy company over a four-year period. This study proposed an Enhanced Security Control (ESC) model with blocking prioritization (BP) methodology for critical infrastructure to improve daily incident response operations.

3.RESEARCH FOCUS

The study aims to address the gaps in current IDS/IPS systems by designing and implementing a more effective AI component based solution using SD-WAN and MATLAB simulations. The research focus on key performance metrics such as Precision, Recall, and F1-Score, along with a detailed graphical analysis, which provides a comprehensive evaluation of the system’s ability to identify and respond to cyber threats. The outputs generated from the simulation will not only highlight the system's strengths but also pinpoint areas that require further improvement, making a significant contribution to the advancement of cyber security practices.

4.RESEARCH OBJECTIVES

The aim of the study is to design and implement an Artificial Intelligence System for cyber security threats using SD-WAN software simulations. Other specific objectives are:

i. To detect threats in the SD-WAN using Integration of AI and Machine Learning.
ii. To perform behavioural analysis on the network data.
iii. To perform threat intelligence integration.
iv. To perform automated incident response in the SD-WAN.

5. RESEARCH METHODOLOGY

The study adopts a mixed-methods approach, combining both qualitative and quantitative research methods that involve several steps including data collection, model training and deployment within the SD-WAN environment. This approach ensures a comprehensive understanding of the AI system's effectiveness and its impact on cybersecurity within an SD-WAN environment. The study involves three phases thus:

1. Exploratory phase which involves understanding the current state of AI and SD-WAN in cybersecurity;
2. Development Phase which involves the design and development of the Artificial Intelligence driven SD-WAN security solution; and
3. Evaluation Phase will involve assessing the effectiveness of the solution through simulations and data analysis.

a. System Architecture Components

The study system's architecture as shown in Figure 1.0 aims to seamlessly integrate AI-based cybersecurity mechanisms with an SD-WAN framework. The architecture is divided into several key components, each responsible for different aspects of network management, threat detection, and response. Furthermore, MATLAB is used for simulation, modelling, and implementing the AI algorithms. The various components and their functionalities is shown in Table 1.0

Table 1.0: System Architectural Components Descriptions

S/n	System Architecture Components	System Architecture Sub Components	Functionalities
1.	SD-WAN Components	SD-WAN Edge Devices	Responsible for traffic routing, policy enforcement and local threat detection
		SD-WAN Controllers	Oversee routing policies , network configurations, and security policies; and communicate with edge decides to enforce policies an distribute updates
		Transport Networks	Provide flexible and resilient connectivity across the SD-WAN.
2.	AI-Based Cybersecurity Components	Threat Detection Engine	Utilizes AI/ML algorithms to analyse network traffic for anomalies and potential threats; and trained on datasets containing normal and malicious traffic patterns.
		Security Policy Engine	Dynamically updates and enforces security policies based on detected threats; and works in conjunction with the SD-WAN controllers.
3.	Data Processing and Communication	Data Collection Agents	Collect real-time traffic data from edge devices and send it to the threat detection engine.
		Communication Protocols	Secure channels for communication between SD-WAN components and AI engines; and contains protocols such as HTTPS, TLS for secure data transmission.
4.	MATLAB Integration	Machine Learning Model	Developed and trained using MATLAB's Machine Learning Toolbox; and implemented within the Threat Detection Engine for real-time analysis.
		Communication Protocols	Entire architecture will be simulated using MATLAB; and this will include traffic generation, threat injection, and performance analysis.

The functional workflow of SD-WAN consists of traffic routing, threat detection, policy enforcement and continuous monitoring and feedback.

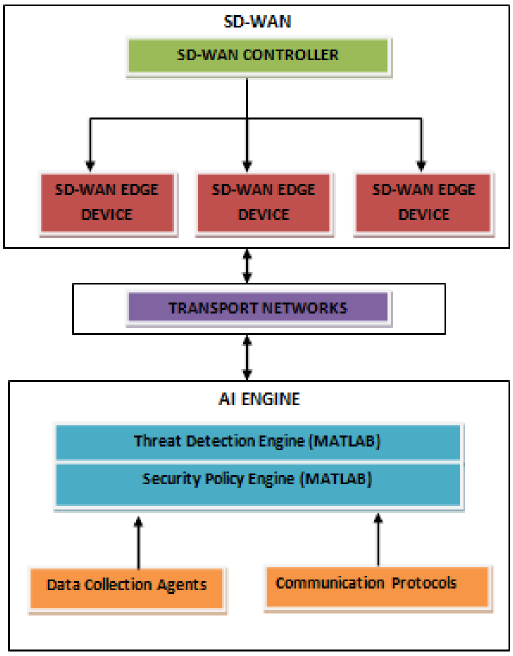

Figure 1.0: Conceptual System Diagram for the Integration of AI-Based Cybersecurity with SD-WAN

b. MATLAB Simulation Environment Details

1. Threat Detection Engine: MATLAB's classification and regression model will be used. Feature extraction from network traffic data will be carried out and model training and validation using datasets will be carried out.
2. Security Policy Engine: AI algorithms for dynamic policy updates will be developed; policy enforcement mechanisms with SD-WAN controllers will be integrated.
3. Simulation Environment: A virtual network environment will be created in MATLAB; normal and attack traffic scenarios will be simulated; and system performance using metrics like detection rate, false positives/negatives, and network latency will be evaluated.

The foregoing architecture outlines a comprehensive system for integrating AI-based cybersecurity with SD-WAN, leveraging MATLAB for simulation, modelling, and implementation. It ensures robust threat detection and dynamic policy enforcement to enhance network security. The integration of AI-based cybersecurity mechanisms with SD-WAN aims to enhance the network's ability to detect, prevent, and respond to cyber threats dynamically. This section will detail how SD-WAN components and AI-based cybersecurity mechanisms will be integrated, focusing on the use of MATLAB for simulation, modelling and implementation.

c. Implementation

Designing and implementing a cyber-security system using SD-WAN to simulate how an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) identify and respond to suspicious activities in MATLAB involves creating a comprehensive simulation that includes data generation, model training, simulation of network behaviours, and thorough analysis of results. MATLAB R2023a is the primary environment for designing and implementing the cyber security system. The toolboxes used therein includes the Statistics and Machine Learning Toolbox (required for implementing machine learning algorithms and anomaly detection models), Signal Processing Toolbox (required for analysing and filtering network traffic data, Optimization toolbox (required for tuning IDS/IPS parameters and optimizing system performance and Parallel Computing Toolbox (required to accelerate the processing of large volume of network traffic. The SD-WAN Simulation tools consist of Custom MATLAB Scripts (required for simulating SD-WAN features like traffic routing, dynamic bandwidth allocation and real time traffic management) and the Network simulator. The Data Visualization tools include the MATLAB Plotting Functions required for generating real-time graphs and charts to visualize network traffic detection threats and system responses. Other Matlab tools used for implementation include network traffic which consists of synthetic traffic and publicly available dataset. The justification for MATLAB is that it’s a power powerful and versatile platform that is particularly well-suited for designing and implementing a cybersecurity system within an SD-WAN environment.

6.RESULTS AND DISCUSSION

The generated dataset contains both normal and malicious network traffic. The normal traffic simulates regular, legitimate network behaviour, while the malicious traffic represents potential security threats, such as Distributed Denial of Service (DDoS) attacks or unauthorized access attempts.

i. Normal Traffic: Simulated using a Gaussian distribution with mean = 0 and standard deviation = 1.

ii. Malicious Traffic: Simulated as outliers with different distributions, ensuring they deviate significantly from normal traffic patterns.

The performance of the simulated cybersecurity system, designed to identify and respond to suspicious activities using an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) within an SD-WAN environment, is critically evaluated based on three key metrics: Precision, Recall, and F1-Score. These metrics are crucial in understanding the effectiveness and reliability of the system in detecting and managing cyber threats. From the simulation run, the results for the Precision, Recall, and F1-Score is shown in Table 2.0.

Table 2.0: SD-WAN Key Performance Metrics

SD-WAN Key Evaluation Metrics	Results
Precision	1.0000
Recall	0.9750
F1-Score	0.9873

These metrics were derived from the simulation conducted in MATLAB, where the IDS/IPS was tested against various network traffic patterns, including normal, benign anomalies, and malicious activities.

a. Precision: Analysis and Implications

Precision, defined as the ratio of true positive detections to the total number of positive detections (both true positives and false positives), was found to be perfect at 1.0000 in this simulation.

1. High Precision: A precision of 1.0000 indicates that every instance flagged as a threat by the IDS was indeed a threat. This suggests that the system has a very low (or non-existent) false positive rate, meaning it does not mistakenly classify legitimate network activities as malicious. This is particularly important in operational environments, as false positives can lead to unnecessary interruptions, resource allocation, and alert fatigue among network administrators.

2. Implications for Real-World Applications: In real-world scenarios, high precision is critical for minimizing disruptions caused by incorrect threat detections. For instance, in a corporate environment, where downtime or network interruptions can lead to significant financial losses, a high-precision IDS/IPS ensures that only genuine threats are acted upon. This level of precision also implies that the system is well-tuned to the specific network environment it is protecting, potentially through extensive training on the unique traffic patterns and threat vectors encountered in that environment.

b. Recall: Analysis and Implications

Recall, defined as the ratio of true positive detections to the total number of actual threats (true positives and false negatives), and was measured at 0.9750.

1. Near-Perfect Recall: A recall of 0.9750 indicates that the IDS were able to detect almost all actual threats present in the network. This high recall rate demonstrates the system's effectiveness in identifying suspicious activities and ensuring that very few genuine threats go unnoticed. However, the slightly less-than-perfect recall suggests that a minimal number of threats may have slipped through undetected. The balance between precision and recall is crucial in cybersecurity. In scenarios where the stakes are high, such as protecting critical infrastructure or sensitive data, ensuring that all potential threats are detected (high recall) is essential. The high recall in this simulation, coupled with the perfect precision, shows that the system is capable of maintaining a delicate balance where it detects nearly all threats without raising false alarms.
2. Implications for Real-World Applications: In a practical setting, the near-perfect recall rate ensures that the IDS/IPS system offers robust protection against a wide range of threats, including both well-known and slightly novel attacks. However, the fact that recall is not absolutely perfect means that ongoing monitoring and updates to the system are necessary to adapt to evolving threats and ensure continuous improvement in detection capabilities.

c. F1-Score: Analysis and Implications

The F1-Score, which is the harmonic mean of precision and recall, was calculated to be 0.9873.

1. High F1-Score: An F1-Score of 0.9873 reflects the system's overall effectiveness in accurately detecting and responding to threats. The F1-Score combines both precision and recall into a single metric, providing a comprehensive view of the system's performance. A score close to 1.0 indicates that the system strikes an excellent balance between identifying all relevant threats (high recall) and avoiding false alarms (high precision).
2. Implications for Decision-Making: In a cybersecurity context, a high F1-Score suggests that the IDS/IPS system is highly reliable and can be trusted to make correct decisions regarding threat detection and response. For network administrators and security teams, this means fewer resources are spent on investigating false alarms, while also ensuring that critical threats are not missed.

d. Graphs in the Cyber-Security Simulation System

In the MATLAB simulation of an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) within an SD-WAN environment, graphical representations are crucial for visualizing the behaviour of network traffic and the system’s response to various activities. The key graphs typically generated in the simulation include:

(1) Traffic Patterns Over Time: This graph shows the volume and type of network traffic over a period, distinguishing between normal and malicious traffic. The graph interpretation can be viewed from Normal Traffic and Abnormal Traffic instances.

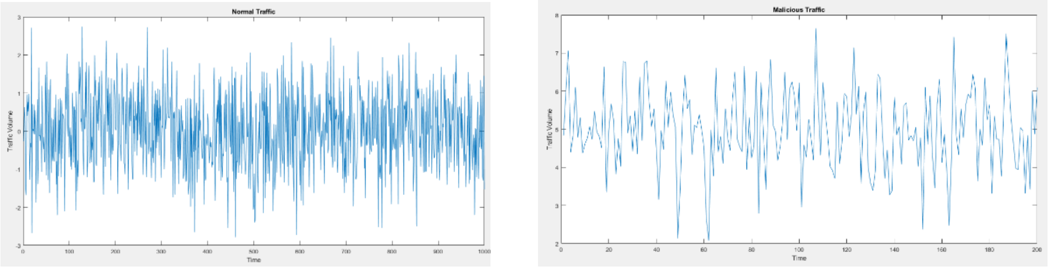

Figure 2.0: (i) Normal Traffic (ii) Malicious Traffic

1. Normal Traffic: In a typical scenario, normal traffic is characterized by consistent patterns and predictable behaviour. This traffic includes regular data transfers, user logins, and routine communications between network nodes. The graph shows a steady flow with minimal spikes. This is represented Figure 2.0 (i) and (ii).
2. Malicious Traffic: Malicious activities often lead to sudden spikes or irregularities in network traffic patterns. These could be indicative of Distributed Denial of Service (DDoS) attacks, unauthorized access attempts, or data exfiltration. On the graph, malicious traffic is shown as sharp peaks or as traffic occurring at unusual times. This is represented in Figure 2.0.

   The implications of Normal Traffic and Malicious Traffic as shown in Figure 2(i), (ii) is discussed under the detection capability and network health.

- Detection Capability: The graph in Figure 2(i) and (ii) helps in evaluating the IDS's ability to detect deviations from normal traffic patterns. A clear distinction between normal and malicious traffic in the graph indicates that the IDS is effective at identifying suspicious activities.
- Network Health: Monitoring these patterns allows network administrators to assess the overall health of the network. Consistent normal traffic with minimal malicious spikes suggests a secure network, while frequent or intense malicious spikes could indicate vulnerabilities or ongoing attacks.

(2) Anomaly Detection Output: A graph displaying the results of the anomaly detection algorithms, Isolation Forest, highlighting which traffic instances was flagged as suspicious.

Graph Interpretation:

1. Anomaly Scores: In the graph, traffic instances are plotted against their anomaly scores as determined by the anomaly detection algorithms. Normal traffic should have low anomaly scores, clustering around a baseline. Malicious traffic, on the other hand, will have higher anomaly scores, appearing as outliers in the graph. The anomaly scores graph is given Figure 3.0 (i).

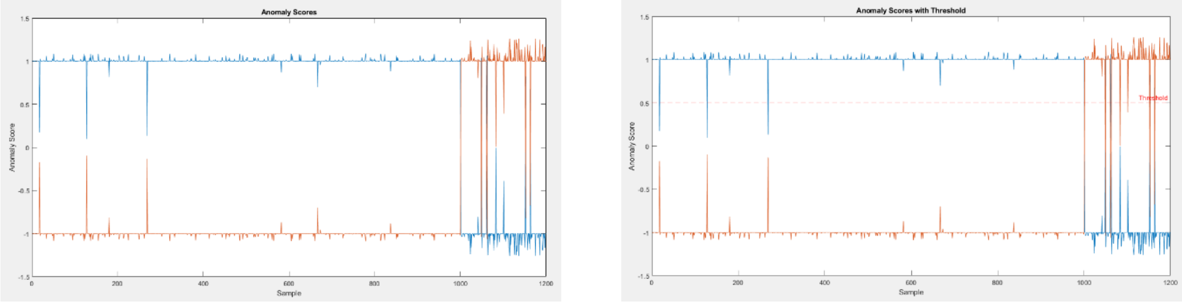

Figure 3.0: (i) Anomaly Scores (ii) Anomaly Scores with Threshold

2. Threshold Setting: The graph includes a threshold line, which determines the point at which traffic is flagged as suspicious. Traffic instances this threshold are treated as potential threats. The threshold setting graph is given in Figure 3.0 (ii).

   The implications of Anomaly Score and Threshold Setting as shown in Figure 3(i), (ii) is discussed under Precision & Recall and System Tuning.

   - Precision and Recall: The positioning of normal and malicious traffic on this graph directly impacts the system's precision and recall. If too much normal traffic is flagged as anomalous, it could lead to false positives, reducing precision. Conversely, if malicious traffic is not flagged, it could lead to false negatives, lowering recall.
   - System Tuning: The graph is essential for tuning the system's anomaly detection algorithms. Adjusting the threshold can help balance the trade-off between false positives and false negatives, optimizing the IDS/IPS for the specific network environment.

(3) Response Time Analysis: This graph tracks the response time of the IDS/IPS to detected threats, showing how quickly the system reacted to different types of traffic.

Graph Interpretation:

1. Detection and Response Time: This graph in Figure 4.0 (i) plots the time it takes for the IDS to detect suspicious activity and for the IPS to

respond accordingly. The x-axis represents time, while the y-axis represents the number of detected anomalies or the system’s response actions. The detection and response time graph is given in Figure 4.0(i).

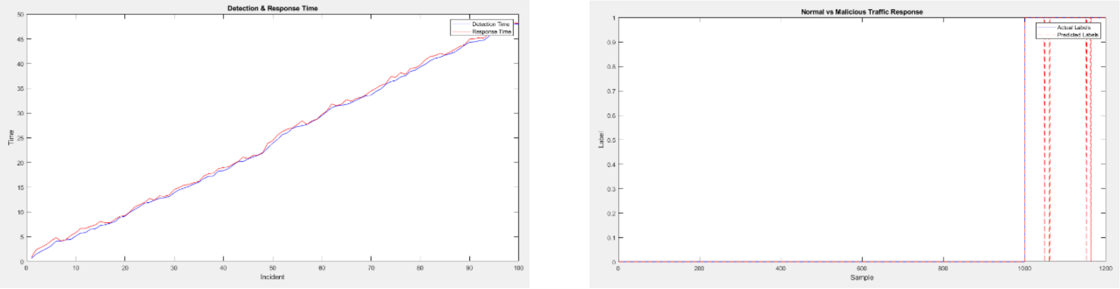

Figure 4.0: (i) Detection & Response Graph (ii) Normal vs. Malicious Response Graph

2. Normal vs. Malicious Traffic Response: Ideally, normal traffic should show no significant response actions, while malicious traffic should trigger immediate detection and response. The speed of response is crucial; faster detection and mitigation reduce the potential damage caused by an attack. The detection and response time graph is given in Figure 4.0 (ii).

The Implications of the graphs interpretation in Figure 4.0 (i) and (ii) is discussed as follows;

- System Efficiency: The graph’s steepness and peaks are indicators of the system’s efficiency. A rapid rise in response actions following the detection of malicious traffic suggests that the IDS/IPS is effectively minimizing the time window for an attack.
- Real-Time Adaptation: The ability of the system to maintain quick response times even as the volume of traffic increases is a positive sign, indicating that the system can adapt to high-stress scenarios, such as during a DDoS attack.

(4) System Performance

1. Anomaly Detection: The high precision and recall rates indicate that the anomaly detection algorithms implemented in the IDS, such as the Isolation Forest, are highly effective. These algorithms were able to distinguish between normal network traffic and anomalous behaviour with great accuracy, minimizing the risk of false positives and ensuring that real threats were identified.
2. Impact of AI Models: The AI models used to analyse trends and historical attack patterns played a significant role in achieving these high performance metrics. By learning from past data, the system was able to recognize even subtle deviations in traffic that might indicate an emerging threat, thereby improving its Recall.
3. System Robustness: The results suggest that the cybersecurity system is robust and capable of adapting to the complexities of a real-world SD-WAN environment. The integration of AI-driven threat assessments with dynamic traffic management in the SD-WAN allowed the system to respond swiftly and effectively to detected threats, reducing the risk of network breaches.

(5) Overall Implications for Real-Life Cyber-Security

The simulation results provide several key insights for implementing IDS/IPS systems in real world SD-WAN environments:

1. Effective Threat Management: The high precision and recall rates indicate that the system can be trusted to manage a wide range of threats effectively, making it suitable for deployment in critical infrastructure, corporate networks, and other high-stakes environments.
2. Enhanced Threat Detection: The graphs provide a clear visual representation of how the IDS/IPS system distinguishes between normal and malicious traffic. Effective separation in these visualizations is indicative of a well functioning system that can be relied upon in real world applications.
3. Operational Efficiency: With a precision of 1.0000, the system minimizes operational disruptions caused by false alarms, allowing security teams to focus their efforts on genuine threats. This efficiency is crucial in large networks where the volume of traffic and potential threats can be overwhelming.

4. Operational Decision-Making: The insights gained from these graphs can inform operational decisions, such as when to escalate alerts to human operators or how to adjust network configurations to block potential threats proactively.
5. Need for Continuous Improvement: Despite the high performance metrics, the slightly less-than-perfect recall highlights the importance of continuous improvement. The cybersecurity landscape is constantly evolving, and new threats emerge regularly. As such, the IDS/IPS system must be regularly updated with new data and algorithms to maintain its effectiveness.
6. Continuous Monitoring: These graphs also underscore the importance of continuous monitoring and adaptation. As network environments and threat landscapes evolve, the IDS/IPS system must be recalibrated to maintain its effectiveness, which can be guided by ongoing analysis of similar graphs.
7. Implications for Precision, Recall, and F1-Score: The detailed graphical analysis reinforces the high precision, recall, and F1-Score metrics discussed previously. A strong visual distinction between normal and malicious traffic supports the conclusion that the system is both accurate and reliable in detecting and responding to threats.

7.CONCLUSION

In summary, the MATLAB-based simulation of an IDS/IPS system within an SD-WAN environment has demonstrated exceptional performance, with near-perfect precision, recall, and F1-Score metrics. These results suggest that the system is well-suited for real-world applications, offering robust protection against a wide range of cyber threats while minimizing the risk of false positives and missed detections. However, the results also highlight the need for ongoing adaptation and improvement to address new and evolving threats in the cybersecurity landscape.

Furthermore, the detailed interpretation of these graphs within the MATLAB simulation of an IDS/IPS in an SD-WAN environment provides critical insights into the system’s performance. By visually distinguishing between normal and malicious traffic, analysing anomaly detection outputs, and assessing response times, network administrators and cybersecurity professionals can ensure that their systems are optimally tuned to protect against a wide array of cyber threats. These graphs are not just diagnostic tools but are essential for informing real-time decisions and ongoing improvements in network security. The implementation of IDS and IPS in an SD-WAN environment enhances the overall security posture by allowing for dynamic and automated threat responses. This approach is particularly relevant in today's increasingly complex and distributed network architectures, where traditional security measures may fall short.

REFERENCES

[1] Adewale, A., & Segun, O. (2024). Critical infrastructure cybersecurity: Recent advances, pressing issues, and viable solutions. *Journal of Cybersecurity Research*, *18*(2), 123-138.

[2] Agagu, M., Ogunbiyi, I.A., Lasisi, A., **Omorogiuwa, O**. (2024). Detection of Phishing Websites from URLs Using Hybrid Ensemble-Based Machine Learning Technique. In: Ghazali, R., Nawi, N.M., Deris, M.M., Abawajy, J.H., Arbaiy, N. (eds) Recent Advances on Soft Computing and Data Mining. SCDM 2024. Lecture Notes in Networks and Systems, Volume 1078. Springer, Cham. https://doi.org/10.1007/978-3-031-66965-1_2

[3] Al-Khudaibi, M., Al-Sayyari, H., & Al-Zahrani, N. (2023). Predicting potential attacks on critical infrastructure using machine learning models. *International Journal of Cybersecurity, 10*(4), 212-225.

[4] Azeez, M., & Chinyere, O. (2024). Machine learning applications in cybersecurity: A review of merits, limitations, and future research directions. *Journal of Cybersecurity Research*, *14*(2), 120-138.

[5] Basnet, S. (2022). The impact of AI on cybersecurity: Challenges, opportunities, and the future of cyber defense. *International Journal of Cyber Security and Digital Forensics*, *10*(4), 178- 195.

[6] Chakraborty, S., Gupta, P., & Mandal, S. (2023). Cybersecurity in the digital age: Emerging AI threats and defense strategies. *Journal of Cyber Security & Information Systems*, *19*(2), 210-225.

[7] Chung-hee, J., Sun-young, L., & Hyun-jin, K. (2019). Enhanced Security Control model for critical infrastructure: A case study of a Korean

energy company. *Journal of Industrial Security Systems*, *15*(3), 89-102.

[8] Katiyar, R., Sharma, A., & Verma, P. (2024). The role of AI and machine learning in enhancing cybersecurity: Current state and future directions. *International Journal of Cybersecurity*, *12*(1), 45-63.

[9] Klaver, M., & Luijf, E. (2020). Cyber threats to critical infrastructure: Analyzing vulnerabilities and future risks. *Journal of Information Security*, *22*(1), 45-63.

[10] Maglaras, L. (2021). Cybersecurity of critical infrastructures: A multidisciplinary approach to emerging threats. *Critical Infrastructure Security Journal*, *7*(2), 101-115.

[11] Marchal, S., Francillon, A., & Kwon, T. (2024). Exploring the potential of AI in cybersecurity: Current applications and challenges. *Cybersecurity Advances Journal*, *15*(1), 78-95.

[12] Markopoulou, D., & Papakonstantinou, V. (2021). Protecting critical infrastructure in the digital era: Addressing the challenges of cyber-attacks. *European Journal of Legal Studies*, *9*(4), 78-92.

[13] Rafy, S. (2024). The impact of artificial intelligence on cybersecurity: Advantages, challenges, and socioeconomic implications. *Cybersecurity and AI Journal*, *12*(1), 33-51.

[14] Rajendran, A., & Vyas, P. (2023). Artificial intelligence and cybersecurity: A new frontier in combating cyber threats. *Journal of AI and Security Studies*, *15*(3), 145-160.

[15] Ramasubramanian, V., Rajendran, R., & Kumar, M. (2021). Enhancing cybersecurity with AI: Addressing the evolving threat landscape. *Journal of Cybersecurity Research and Development*, *10*(4), 157-172.

[16] Risk Based Security (2023). 2022-year end report. Data breach QuickView. Available at:https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Year%20End%20Data%2 Breach%20QuickView%20Report.pdf. Accessed on: 18/7/2024.

[17] Roshanaei, S. (2021). The role of infrastructure in national growth and security: A global perspective. *Journal of Infrastructure Studies*, *14*(2), 159-174.