Comprehensive Impact Assessment of Intrusion Detection and Mitigation Strategies Using Support Vector Machine Classification

Oscar Ebong[1], Anthony Edet[2*], Anietie Uwah[3], Ndueso Udoetor[1]
[2]Department of Computer Education and Robotics, University of Uyo, Nigeria.
[1]Department of Computer Science, Akwa Ibom State University, Mkpat Enin, Nigeria.
[3]Department of Computer Science, National Open University of Nigeria, Abuja, Nigeria
oskndott@gmail.com[1], anthonyedet73@gmail.com[2], uwahanietie@gmail.com[3],
Udoetorndueso55@gmail.com[1]

DOI: 10.56201/rjpst.v7.no2.2024.pg50.69

Abstract
Cybersecurity remains a paramount concern in today's interconnected digital space, necessitating continual evaluation and refinement of intrusion detection and mitigation strategies. This study presents a comprehensive impact assessment of various intrusion detection and mitigation methods, adopting Support Vector Machine (SVM) classification for analysis. Through critical examination of diverse techniques, including signature-based, behavior-based, and anomaly-based approaches, the research evaluates their effectiveness in combating cyber threats. Notably, SVM classification achieves an accuracy score of 87%, revealing its utility in discerning subtle patterns indicative of malicious activity. Furthermore, the study highlights the significance of proactive measures such as user training, network segmentation, and multi-factor authentication in fortifying defense mechanisms. By providing valuable insights into the strengths and limitations of different approaches, this work contributes to the ongoing efforts to safeguard digital ecosystems against evolving cyber threats.

Keywords: *Intrusion, SVM, Cyber threats, Network, Mitigation Strategy*

1.0 INTRODUCTION

In today's digitally interconnected world, information security has become a paramount concern for individuals, organizations, and governments alike (Michal and Maurice, 2023). With the proliferation of external intrusion attempts, such as hacking, malware, and phishing attacks, the need for robust security response methods is more critical than ever. Timely and effective responses to external intrusions are essential to mitigate potential damage and safeguard sensitive information. Security response methods play a pivotal role in identifying and addressing external intrusion attempts. These methods encompass various techniques, from signature-based detection to anomaly detection and incident response strategies (Michal and Maurice, 2023). However, the effectiveness of these methods can vary significantly, and choosing the most appropriate response in a given situation is often challenging. Decisions must be made quickly, and a wrong response can have severe consequences (Alamin et al., 2023). The need for carrying out an impact assessment of security response methods in cybersecurity is multifaceted and critical for several reasons. Firstly, it helps evaluate the

effectiveness of the security response mechanisms in place (Alamin et al., 2023). This evaluation is essential to gain insights into how well the chosen methods are performing in mitigating and addressing external intrusion attempts. By understanding the strengths and weaknesses of these methods, organizations can make informed decisions about refining their security strategies. Moreover, an impact assessment is vital for tailoring response strategies to the specific nature of security threats. It acknowledges that different intrusion incidents may require different response approaches. This customization is a key element in ensuring that security measures are adaptive and efficient in the face of diverse and evolving cyber threats (Alamin et al., 2023). A one-size-fits-all approach often falls short in addressing the complexities of modern cybersecurity. Another significant aspect is resource allocation. Cybersecurity resources, which encompass personnel, tools, and budgets, are finite and valuable assets. Conducting an impact assessment aids in allocating these resources effectively. By identifying which response methods have the most substantial impact on mitigating threats, organizations can prioritize investments, optimize resource allocation, and ensure they are addressing the most critical security issues (Edet et al., 2024). In addition, minimizing downtime and damage caused by security incidents is paramount. A timely and appropriate response is pivotal in reducing the potential impact of intrusions, such as data breaches or service disruptions. An impact assessment enables organizations to fine-tune their response strategies, thereby minimizing the severity of incidents and limiting the associated damage (Carrier et al., 2022). Furthermore, enhancing incident recovery is another key facet. Effective recovery from security incidents is a crucial element of cybersecurity. An impact assessment provides insights into the time and effort required for different types of incident recovery. This information helps organizations streamline their recovery processes, reducing downtime and ensuring a swifter return to normal operations (Dener et al., 2022). Lastly, an impact assessment is integral for compliance and reporting purposes. In many industries, organizations are subject to regulations and compliance requirements concerning data protection(Ekong et al., 2023) and cybersecurity. Demonstrating that impact assessments have been conducted and that responses are in place to address potential threats is essential for meeting these obligations and ensuring transparency and accountability in the realm of cybersecurity (Shetty et al., 2020). Machine learning (ML) has emerged as a powerful tool (Ekong et al., 2022) in the field of cybersecurity. It offers the potential to improve the accuracy and efficiency of security response methods by automating decision-making processes. ML models can analyze vast datasets in real-time, detect patterns, and make informed decisions about whether a detected event is a security threat and, if so, how to respond (Alkhatib et al., 2021). Support Vector Machine (SVM) is a popular ML algorithm that excels in classification tasks, making it particularly well-suited for intrusion detection and response assessment. It combines the outputs of multiple decision trees to improve predictive accuracy and reduce the risk of overfitting. The Support Vector Machine (SVM) algorithm has been applied successfully in various domains, including healthcare, finance, and cybersecurity (Kharwar et al., 2022). The research problem at hand is rooted in a multifaceted challenge within the field of cybersecurity. Firstly, there is a significant gap in empirical assessment regarding the impact of machine learning (ML)-informed security response methods on external intrusion incidents. Despite the increasing adoption of ML algorithms for threat detection, a scarcity of in-depth, real-world studies evaluating the actual effectiveness of these response methods leaves a critical knowledge void. This research gap raises fundamental questions about whether organizations are making well-informed choices when integrating ML into their security response strategies. A related concern pertains to the diversity of the threat field. Cyber threats continually evolve and encompass various attack

vectors, each demanding distinct response strategies. The deficiency in tailored response approaches is particularly striking, highlighting the need to address whether current security response methods are adequately adapted to the nuances of different intrusion attempts. This question is crucial, given that a one-size-fits-all response approach often proves inadequate in effectively mitigating today's complex security threats. Resource allocation is yet another significant dimension of this research problem. Cybersecurity resources, such as personnel, tools, and budgets, are finite and valuable. However, without a systematic assessment of the impact of different security response methods, organizations risk misallocating these resources. This misallocation not only compromises incident response capabilities but also undermines the overall cybersecurity posture. In essence, the problem of resource allocation efficiency is intricately linked to the need for assessing response impact, making it a critical component of the research problem. Furthermore, the challenge extends to the need for minimizing downtime and damage caused by security incidents. Timely and effective responses to intrusions are essential for reducing the potential impact of these incidents. An in-depth understanding of how response methods impact downtime and damage mitigation is essential. This aspect underscores the importance of assessing the actual outcomes of security response methods and how they affect the severity and consequences of security breaches.

2.1 THEORETICAL FOUNDATION/BACKGROUND

In this section, the theoretical analysis of Network security, its techniques, its mitigation methods, and work done by several authors with specific focus on Network intrusion are presented.

2.1 OVERVIEW OF CYBERSECURITY

Cybersecurity is a multidisciplinary field dedicated to safeguarding digital systems, networks, and data from unauthorized access, attacks, and damage. In an era dominated by digital transformation and connectivity, the importance of cybersecurity cannot be overstated. The overarching goal of cybersecurity is to ensure the confidentiality, integrity, and availability of information in the face of evolving cyber threats (Kumar et al., 2021). As organizations increasingly rely on interconnected technologies, cybersecurity plays a critical role in preserving trust, privacy, and the overall functionality of digital ecosystems. The field of cybersecurity is dynamic and constantly evolving to counteract the ever-changing tactics employed by malicious actors. It encompasses a wide range of strategies, technologies, and practices designed to protect against a diverse array of cyber threats, including malware, ransomware, phishing attacks, and more. Cybersecurity professionals employ proactive measures such as encryption, firewalls, and intrusion detection systems, as well as reactive strategies for incident response and recovery. Moreover, the human element is crucial in cybersecurity, as awareness, education, and training are essential components of a robust defense against social engineering and insider threats (Kumar et al., 2021). One of the defining characteristics of cybersecurity is its global nature. Cyber threats transcend borders, making international cooperation and information sharing crucial for effectively combating cybercrime. Governments, businesses, and individuals alike must collaborate to establish and adhere to best practices, standards, and regulations that promote a secure and resilient cyberspace. The field of cybersecurity is also marked by ongoing research and development, with experts continuously innovating to stay ahead of emerging threats and vulnerabilities. Despite the advancements in cybersecurity, challenges persist. The rapid pace of

technological innovation introduces new attack vectors, and the increasing sophistication of cyber threats requires a proactive and adaptive approach. Balancing the need for security with user convenience and privacy remains a delicate challenge. Additionally, addressing the global shortage of skilled cybersecurity professionals is an ongoing concern (Kumar et al., 2021). The overview of cybersecurity underscores its pivotal role in preserving the digital field and underscores the need for a holistic, collaborative, and forward-thinking approach to secure our interconnected world. In the contemporary digital field, cybersecurity is not solely a technological concern but also a strategic imperative for organizations across industries. As businesses adopt cloud computing, IoT (Internet of Things), and other transformative technologies, the attack surface for potential cyber threats expands exponentially. Consequently, cybersecurity strategies must be agile and adaptive, integrating risk management principles (Inyang &Umoren, 2023) to identify and prioritize potential threats based on their impact and likelihood. The holistic nature of cybersecurity extends beyond technology to include policies, regulations, and a culture of security awareness that permeates an entire organization. The significance of cybersecurity is underscored by the potential consequences of a successful cyber attack. Beyond financial losses, which can be substantial, organizations face reputational damage and legal repercussions (Elijah et al., 2022). Moreover, critical infrastructure sectors such as energy, healthcare, and finance rely heavily on interconnected systems, making them prime targets for cyber adversaries. The increasing frequency and sophistication of cyber attacks have prompted governments and regulatory bodies worldwide to enact stringent cybersecurity standards to protect both public and private interests. Cybersecurity is a constantly evolving field that requires continuous learning and adaptation. Threat actors continually refine their tactics, techniques, and procedures (TTPs), necessitating a proactive and collaborative approach among cybersecurity professionals. Threat intelligence sharing, both within industries and across borders, is a key component of this strategy (Elijah et al., 2022). Moreover, the integration of artificial intelligence and machine learning in cybersecurity tools has become pivotal for the rapid detection and mitigation of emerging threats. This intersection of technology and human expertise defines the modern cybersecurity field. The overview of cybersecurity encompasses a vast and interconnected set of principles, technologies, and practices aimed at preserving the integrity of digital systems. It is a dynamic and challenging field that demands constant vigilance, innovation, and collaboration to stay one step ahead of cyber threats. As societies become increasingly dependent on digital technologies, the resilience of our interconnected world relies on the effectiveness of cybersecurity measures in mitigating risks and securing the future of a digitally-driven global economy.

2.2 NETWORK SECURITY

Network security is a critical component of the broader field of cybersecurity, focusing specifically on the protection of computer networks and the data they transmit. In the interconnected digital field, where information is constantly exchanged between devices, maintaining the confidentiality, integrity, and availability of data is paramount. Network security encompasses a range of strategies, technologies, and policies designed to safeguard networks from unauthorized access, data breaches, and malicious activities (Edet & Ansa, 2023). One fundamental aspect of network security is the establishment of access controls. This involves implementing measures such as firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs) to regulate and monitor network traffic. Firewalls act as a barrier between a trusted internal network and untrusted external networks,

filtering incoming and outgoing traffic based on predetermined security rules. Intrusion detection and prevention systems identify and respond to potential security threats, while VPNs secure data transmissions over public networks, ensuring the confidentiality of sensitive information (Edet et al., 2024). Encryption plays a pivotal role in network security by transforming data into unreadable formats that can only be deciphered by authorized parties (Sivamohan et al., 2023). Secure communication protocols, such as HTTPS, utilize encryption to protect the confidentiality of data exchanged between web servers and clients. Additionally, virtual LANs (VLANs) are employed to segregate network traffic, enhancing security by isolating different segments of the network and restricting access to sensitive areas. Network security extends to wireless networks, where the implementation of robust authentication protocols, like WPA3 for Wi-Fi networks, is crucial. This prevents unauthorized access and safeguards against common wireless attacks, such as man-in-the-middle attacks and eavesdropping. Beyond technology, network security also involves comprehensive policies and procedures, including regular security audits, employee training, and incident response plans. These measures contribute to a proactive defense against emerging threats and vulnerabilities. Despite continuous advancements in network security, challenges persist, and the field is ever-evolving (Sivamohan et al., 2023). The emergence of sophisticated cyber threats, the increasing complexity of network infrastructures, and the growing reliance on cloud services highlight the need for ongoing innovation and adaptability in network security strategies. As organizations continue to expand their digital footprints, the importance of network security remains a cornerstone in ensuring the resilience and integrity of information systems in the face of evolving cyber threats. Intrusion prevention is a critical aspect of network security, involving the deployment of techniques to detect and thwart potential security breaches in real-time. Intrusion Prevention Systems (IPS) analyze network traffic for malicious activity, using predefined rules and policies to identify and block threats before they can compromise the network. These systems work in tandem with intrusion detection systems, providing a proactive defense mechanism against a wide range of cyber threats, including malware, denial-of-service attacks, and other malicious activities. Network security also involves robust authentication mechanisms to ensure that only authorized users can access network resources. Multi-factor authentication (MFA) has become a standard practice, requiring users to provide multiple forms of identification, such as passwords, biometrics, or security tokens. This adds an extra layer of defense against unauthorized access, especially in scenarios where stolen credentials are a prevalent threat (Sivamohan et al., 2023).

Secure network architecture design is another crucial element of network security. This involves structuring the network in a way that minimizes vulnerabilities and limits the potential impact of a security breach. Concepts such as the principle of least privilege and network segmentation contribute to creating a more resilient network infrastructure. By restricting access based on user roles and segmenting the network into isolated zones, organizations can contain and mitigate the impact of a security incident. Continuous monitoring and threat intelligence are integral components of effective network security. Security Information and Event Management (SIEM) systems aggregate and analyze log data from various network devices, enabling the identification of anomalous patterns or potential security incidents. Additionally, threat intelligence feeds provide up-to-date information on emerging threats, allowing organizations to adapt their security measures in response to evolving cyber risks. Network security is a multifaceted discipline that requires a holistic approach to protect the integrity, confidentiality, and availability of data within interconnected systems. From the implementation of access controls and encryption to

intrusion prevention systems, secure architecture design, and ongoing monitoring, network security is an ongoing effort to stay ahead of the dynamic and sophisticated nature of cyber threats (Sivamohan et al., 2023). As organizations navigate the digital field, investing in robust network security measures remains essential for safeguarding sensitive information and maintaining the trust of users and stakeholders.

2.3 EXTERNAL NETWORK INTRUSION

External network intrusion represents a persistent and dynamic threat field where malicious actors seek to compromise the security of a network from outside its established perimeters. One common avenue for such intrusion is through phishing and social engineering tactics (Carrier et al., 2022). Attackers craft deceptive emails, messages, or websites to manipulate individuals into revealing sensitive information. By obtaining usernames and passwords, attackers can exploit this information to gain unauthorized access to the network, potentially leading to data breaches and system compromise. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are another facet of external network security intrusion. These attacks aim to overwhelm network resources, rendering them unavailable to legitimate users. By flooding the target network with a deluge of traffic, attackers disrupt critical services, causing downtime and financial repercussions for organizations. Preventing and mitigating the impact of these attacks require robust network architecture design and the implementation of countermeasures such as traffic filtering and load balancing (Carrier et al., 2022).

Exploiting vulnerabilities in software, operating systems, or network devices is a prevalent strategy in external network security intrusion. Attackers target weaknesses in outdated software, unpatched systems, or misconfigured settings to gain unauthorized access. Regularly updating and patching systems, conducting vulnerability assessments, and employing intrusion detection systems are crucial components of a proactive defense against these types of intrusions. Zero-day exploits and Advanced Persistent Threats (APTs) represent advanced tactics employed in external network security intrusion. Zero-day exploits take advantage of vulnerabilities that are unknown or not yet patched by vendors, allowing attackers to infiltrate the network undetected (Carrier et al., 2022). APTs, on the other hand, involve sophisticated and targeted attacks often orchestrated by well-funded adversaries with specific objectives such as corporate espionage or data theft. Detecting and responding to these advanced threats necessitates advanced security measures, including threat intelligence analysis, behavior-based anomaly detection, and continuous monitoring. External network security intrusion is a multifaceted challenge that demands a comprehensive and adaptive approach to defense. Organizations must prioritize cybersecurity measures such as user education, regular software updates, robust access controls, and advanced threat detection mechanisms to thwart the evolving tactics of external attackers and safeguard the integrity and confidentiality of their networks (Carrier et al., 2022).

2.4 VULNERABILITIES IN NETWORK SECURITY

Threats and vulnerabilities in network security represent the potential risks and weaknesses that malicious actors may exploit to compromise the integrity, confidentiality, and availability of data within a computer network. Understanding these threats and vulnerabilities is essential for developing effective countermeasures to protect against cyber

attacks (Uwah & Edet, 2024). Here's an overview of common threats and vulnerabilities in network security (Alkhatib et al., 2021):

1. Weak Authentication:

Weak authentication mechanisms, such as easily guessable passwords or lack of multi-factor authentication, create vulnerabilities that attackers can exploit to gain unauthorized access to network resources.

2. Unpatched Software:

Failure to promptly apply security patches and updates to operating systems, applications, and network devices leaves systems susceptible to exploitation. Attackers often target known vulnerabilities that have not been remediated .

3. Insecure Network Protocols:

The use of insecure or outdated network protocols can expose vulnerabilities. Transitioning to secure communication protocols, such as using HTTPS instead of HTTP, helps protect data in transit.

4. Lack of Encryption:

Failing to encrypt sensitive data, both in transit and at rest, leaves it vulnerable to interception and unauthorized access. Encryption helps protect the confidentiality of data even if it falls into the wrong hands (Alkhatib et al., 2021).

5. Poorly Configured Firewalls and Access Controls:

Incorrectly configured firewalls and access controls can create openings for unauthorized access or compromise the effectiveness of security measures. Regularly reviewing and updating firewall rules is crucial for maintaining a secure network perimeter.

6. Unsecured IoT Devices:

The proliferation of Internet of Things (IoT) devices introduces new vulnerabilities. Insecure IoT devices with weak security measures can be exploited to gain unauthorized access to the network or launch attacks from within (Ekong et al., 2021)).

7. Social Engineering:

Social engineering exploits human psychology to manipulate individuals into divulging sensitive information. This can include tactics such as impersonation, pretexting, or baiting to deceive users and gain access to the network.

Mitigating these threats and vulnerabilities requires a comprehensive and proactive approach to network security. This includes implementing strong access controls, regularly updating and patching software, educating users about security best practices, and leveraging advanced security technologies to detect and respond to potential incidents. Regular risk assessments and security audits are also essential for identifying and addressing evolving threats in a dynamic cybersecurity field.

2.5 CYBER THREATS

In the field of cybersecurity, intrusion refers to any unauthorized or unwanted access, manipulation, or compromise of computer systems, networks, or data. The act of intrusion is typically carried out by malicious actors with the intent to exploit vulnerabilities, gain

unauthorized access to sensitive information, disrupt services, or carry out other nefarious activities (Elijah et al., 2022). Understanding the various types of intrusions is crucial for developing effective defense mechanisms and response strategies in the ever-evolving field of cyber threats.

1.Unauthorized Access Intrusions:
Unauthorized access intrusions involve an attacker gaining entry to a system or network without proper authorization. This type of intrusion often exploits weaknesses in authentication mechanisms, such as weak passwords, unpatched software vulnerabilities, or inadequate access controls. Once inside, the attacker may attempt to escalate privileges, move laterally within the network, or exfiltrate sensitive data (Abdulganiyu et al., 2023).

2. Malware-Based Intrusions:
Malware, short for malicious software, is a common vehicle for intrusions. Malware-based intrusions involve the deployment of harmful software, including viruses, worms, trojans, ransomware, and spyware, to compromise systems. These intrusions can occur through infected email attachments, malicious websites, or compromised software installations, leading to a range of consequences, from data theft to system disruptions.

3. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Intrusions:
DoS and DDoS intrusions aim to disrupt the normal functioning of a system, network, or service by overwhelming it with a flood of traffic. In a DoS attack, a single source generates the traffic, while DDoS attacks involve multiple sources. These intrusions can lead to service unavailability, making it challenging for legitimate users to access resources (Abdulganiyu et al., 2023).

4. Insider Threat Intrusions:
Insider threat intrusions involve individuals within an organization exploiting their access privileges for malicious purposes. This can include employees, contractors, or other trusted entities who intentionally or unintentionally compromise security. Insider threats may involve the theft of sensitive data, sabotage, or the facilitation of external attacks.

5. Phishing and Social Engineering Intrusions:
Phishing and social engineering intrusions rely on manipulating individuals into divulging sensitive information or performing actions that compromise security. These attacks often involve deceptive emails, messages, or phone calls that impersonate trusted entities. Once successful, attackers can gain access to credentials or exploit trust to carry out further intrusions (Abdulganiyu et al., 2023).

6. Zero-Day Exploits and Advanced Persistent Threats (APTs):
Zero-day exploits target vulnerabilities in software that are unknown to the vendor or have not yet been patched. APTs are sophisticated and prolonged intrusion campaigns orchestrated by well-funded and organized attackers. These intrusions often involve a combination of multiple attack vectors and are designed to persist over an extended period, evading detection.

7. Credential Theft:

Cyber attackers often target user credentials through various means, such as phishing, keylogging, or credential stuffing attacks. Once obtained, stolen credentials can be used to gain unauthorized access to systems, networks, or sensitive data.

8. Internet of Things (IoT) Vulnerabilities:
The increasing connectivity of IoT devices introduces new attack vectors. Insecure IoT devices can be compromised, leading to unauthorized access, data breaches, or even the disruption of critical infrastructure.

9. Supply Chain Attacks:
Cybercriminals may target the supply chain to compromise software or hardware before it reaches end-users. This tactic allows attackers to distribute malicious components widely and compromise multiple systems simultaneously.

2.6 RELATED WORKS

Michal and Maurice, 2023, proposed a research work on a Review Of Enhancing Intrusion Detection Systems For Cybersecurity Using Artificial Intelligence (AI). The study aims to explore the potential of Artificial Intelligence (AI) in enhancing the IDS's ability to identify and classify network traffic and detect anomalous behavior. The paper offers a concise overview of IDS and AI and examines the existing literature on the subject, highlighting the significance of integrating advanced language models for cybersecurity enhancement. The research outlines the methodology employed to assess the efficacy of AI within IDS. Furthermore, the study considers key performance metrics such as detection accuracy, false positive rate, and response time to ensure a comprehensive evaluation. Findings indicate that AI is a valuable asset in enhancing the accuracy of AI for detecting and responding to cyber attacks. However, the authors did not state which response approach is suitable for a given scenario. They did not also mention which security response approach is the best given their studies. In the new work, we propose to design a system that examines intrusion response approach and determine which one has the best impact, and also predict a response approach based on a given intrusion scenario.
Talukder et al., 2023 made a research on A Dependable Hybrid Machine Learning Model for Network Intrusion Detection. In this research, the authors proposed a new hybrid model that combines machine learning and deep learning to increase detection rates while securing dependability. The method ensures efficient pre-processing by combining SMOTE for data balancing and XGBoost for feature selection. they compared the developed method to various machine learning and deep learning algorithms in order to find a more efficient algorithm to implement in the pipeline. Furthermore, they chose the most effective model for network intrusion based on a set of benchmarked performance analysis criteria. their method produces excellent results when tested on two datasets, KDDCUP'99 and CIC-MalMem-2022. However, their assessment of effectiveness was algorithm based and was not based on the impact of the model on the intrusion problem handled. We need a system that accuracy is measured based on impact of the model on the situation, and not just on the performance of the algorithm on the dataset supplied.
Kumar et al., 2021, The article provides an overview of the evolving field of network threats and the various security mechanisms employed to safeguard networks, including firewalls, antivirus software, and intrusion detection systems (IDS). Specifically, it focuses on network-based intrusion detection systems (NIDS) and reviews research trends, approaches, and

commonly used datasets for evaluating IDS models. The analysis is based on citation counts, publication trends, and the most cited research articles in the field. By examining the state-of-the-art NIDS, popular techniques, and benchmark datasets, the article offers insights valuable for both novices and researchers interested in understanding the dynamics of NIDS research and its applications.

Maseno et al., 2022, The research addresses the critical need for ensuring the confidentiality, integrity, and availability of information systems amid the rapid expansion of computer networks. It highlights the widespread use of intrusion detection systems (IDSs) as vital tools for network monitoring and security. However, it identifies two primary challenges faced by current IDSs: high rates of false-positive alerts and low detection rates for zero-day attacks. To mitigate these challenges, the study emphasizes the necessity for intrusion detection techniques capable of learning and effectively identifying intrusions. It reviews 111 relevant studies conducted between 2012 and 2022, focusing on hybrid detection systems that integrate machine learning techniques. These hybrid approaches aim to capitalize on the strengths of individual detection methods while addressing their weaknesses. The paper underscores the existing gaps in hybrid intrusion detection system development and advocates for further research in this domain to enhance network security measures.

Abdulganiyu et al., 2023, The research addresses the escalating importance of safeguarding sensitive individual and corporate data traversing the internet against potential intrusions. With security system vulnerabilities, attackers exploit networks to gain unauthorized access to crucial information, posing threats to system operations and data confidentiality. Intrusion detection systems (IDSs) play a pivotal role in cybersecurity by monitoring and analyzing network traffic to identify and report malicious activities. While numerous review papers have explored various intrusion detection approaches, many lack systematic analysis, merely comparing existing techniques without providing in-depth synthesis of methodologies and performance. Moreover, emphasis on anomaly-based IDS, particularly deep-learning models, has overshadowed signature and hybrid-based approaches. Adopting the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) principles, this study comprehensively reviews existing contributions on anomaly-, signature-, and hybrid-based IDS approaches to delineate the state-of-the-art network IDS field. Leveraging data from seven reputable databases, 71 pieces of literature were analyzed and synthesized to address research questions. The findings identify overlooked research areas and unresolved challenges, concluding with recommendations for future research directions aimed at enhancing IDS model efficacy.

Sivamohan et al., 2023, The research investigates the cybersecurity challenges faced by Industry 4.0, which introduces innovative business scenarios like client-specific production and real-time process monitoring but also heightens susceptibility to cyber threats due to resource constraints and system heterogeneity. These threats pose financial losses, reputational damage, and information theft risks. To address these challenges, a novel intrusion detection system called Bidirectional Long Short-Term Memory based Explainable Artificial Intelligence framework (BiLSTM-XAI) is developed. Preprocessing tasks including data cleaning and normalization enhance data quality, while feature selection using the Krill herd optimization (KHO) algorithm identifies significant features from databases. The BiLSTM-XAI approach aims to enhance security and privacy in industrial networks by precisely detecting intrusions. Utilizing SHAP and LIME explainable AI algorithms aids in interpreting prediction results. Experimental evaluations conducted with MATLAB 2016 software using Honeypot and NSL-KDD datasets demonstrate the proposed method's superior performance, achieving a classification accuracy of 98.2% in intrusion detection.

Waleed et al., 2015, This research introduces an innovative software development strategy leveraging Quality of Service (QoS) and parallel technologies within Cisco Catalyst Switches to enhance the analytical capabilities of a Network Intrusion Detection and Protection System (NIDPS) in high-speed network environments. Through real network experiments employing a Snort NIDPS, the study reveals the limitations of NIDPSs, including difficulties processing multiple packets and the tendency to drop packets during periods of heavy traffic without analysis. The research evaluates Snort's analysis performance by assessing metrics such as the number of packets sent, analyzed, dropped, filtered, injected, and outstanding. The findings suggest that incorporating QoS configuration technologies in Cisco Catalyst 3560 Series Switches and deploying parallel Snorts can enhance NIDPS performance and reduce the number of dropped packets. Experimental results indicate notable improvements in performance with this novel configuration approach.

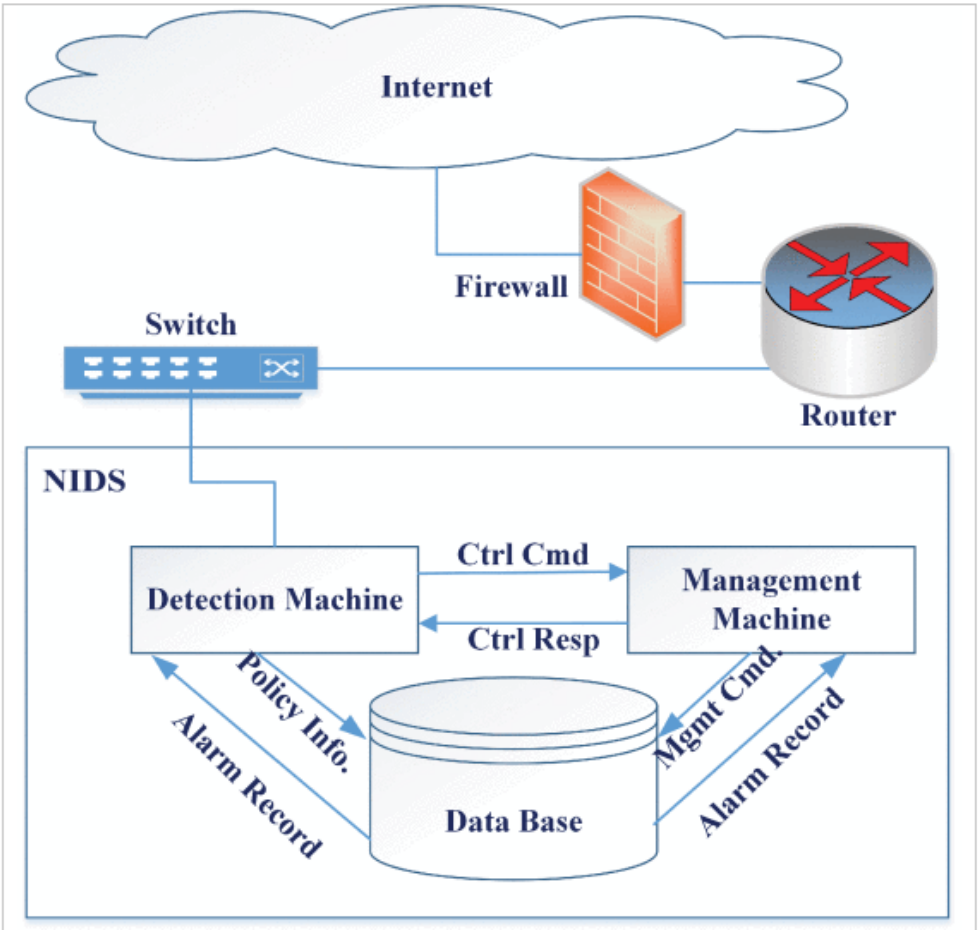

Fig.1 Architecture of the Existing System(Kumar et al., 2021)

3.0 METHODOLOGY

The research problem at hand is rooted in a multifaceted challenge within the field of cybersecurity. Firstly, there is a significant gap in empirical assessment regarding the impact or effect of intrusion on Networks and systems. Despite the increasing adoption of ML algorithms for threat detection, a scarcity of in-depth, real-world studies evaluating the actual effectiveness of these response methods leaves a critical knowledge void. This research gap raises fundamental questions about whether organizations are making well-informed choices

when choosing intrusion detection methods. Examining and analyzing the impact of external network intrusion detection methods is imperative due to the ever-evolving area of cybersecurity threats. With the increasing complexity and sophistication of cyber attacks, organizations must deploy effective intrusion detection systems (IDS) to safeguard their networks and sensitive data. By evaluating the impact of these methods, organizations can make informed decisions regarding the selection and optimization of their security measures. Understanding the effectiveness and efficiency of different IDS approaches is crucial for enhancing network resilience and minimizing the potential damage caused by cyber intrusions.

3.1 SUPPORT VECTOR MACHINE MODEL

In this section, an SVM model for detecting the effect of intrusion on Network systems and classification of the best response method is formulated in steps to ensure sequential flow of the model.

1. Data Representation:
Let (X) represent the feature matrix, where each row corresponds to a sample and each column corresponds to features related to network traffic characteristics and intrusion detection methods. The corresponding class labels are denoted as (y), where (y_i) indicates the impact level of the intrusion detection method (e.g., high impact, moderate impact, low impact).

2. Training SVM:
The SVM aims to find the optimal hyperplane that separates the feature space into regions corresponding to different impact levels of intrusion detection methods (Inyang & Umoren, 2023). This hyperplane is represented as

$$\mathbf{w.\ x + b = 0} \qquad \textbf{(a)}$$

where (w) is the weight vector and (b)is the bias term.

3. Decision Function:
The decision function for SVM is

$$\mathbf{f(x) = w\ .\ x + b} \qquad \textbf{(b)}$$

Depending on the value of (f(x)), the impact level of the intrusion detection method is determined. For example, if (f(x)) is greater than a certain threshold, the method is predicted to have a high impact; if it's between certain bounds, it's predicted to have a moderate impact, and so on.

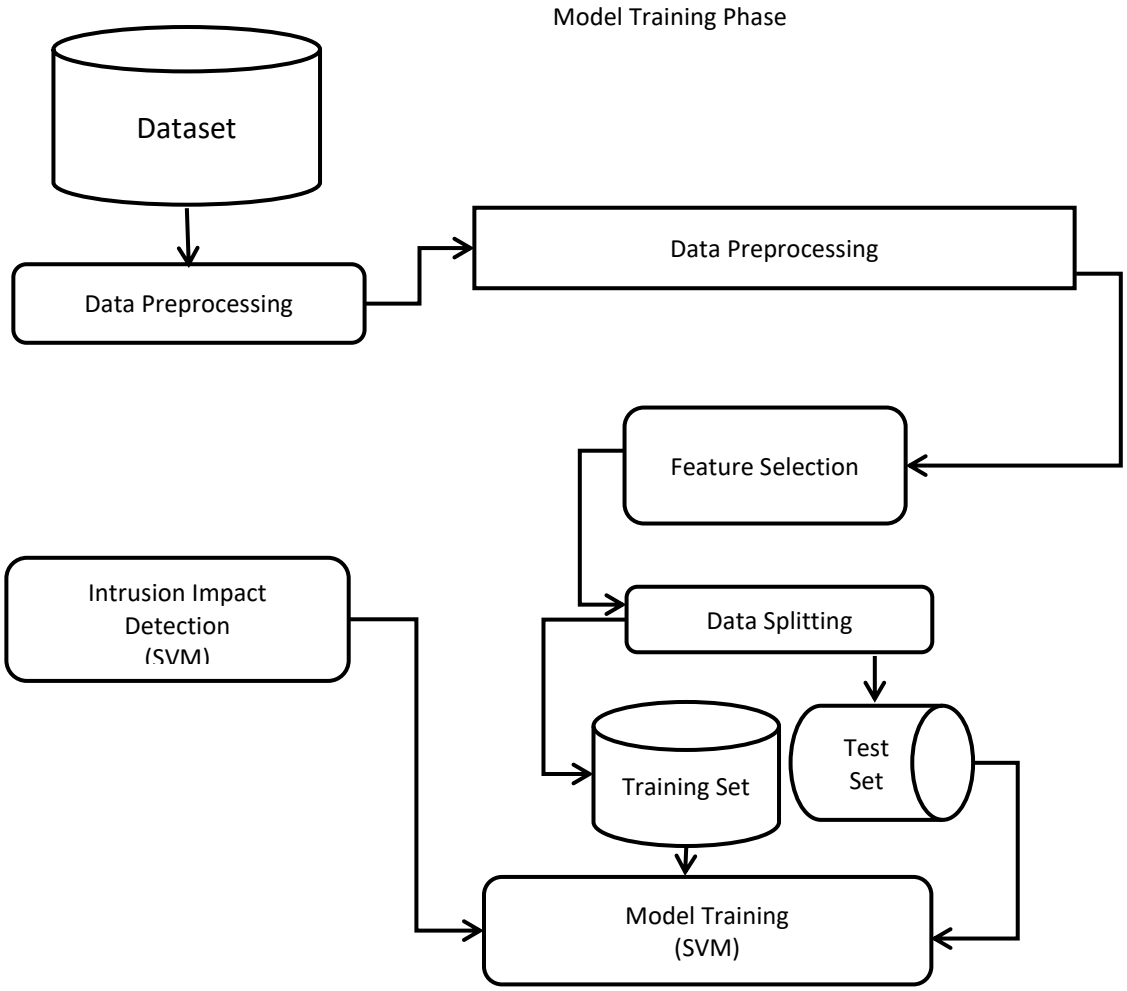

Fig. 2 The Conceptual System Architecture

4.0 RESULTS AND DISCUSSION

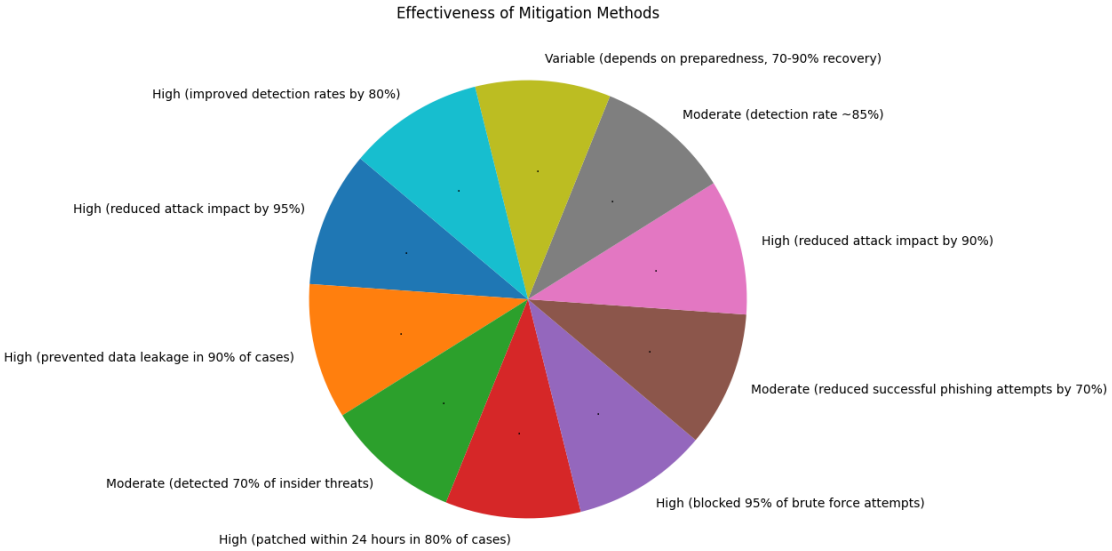

Fig. 3: Piechart Showing Effectiveness of Response Methods

Figure 3 presents a chart illustrating the results of an analysis on various response methods, showcasing their individual performances. This visual representation serves as a valuable tool for decision-making, allowing network administrators to quickly assess and compare the effectiveness of different intrusion response strategies. By providing insights into the relative strengths and weaknesses of each method, Figure 3 enables organizations to tailor their response efforts more effectively, addressing security incidents with targeted and efficient measures.

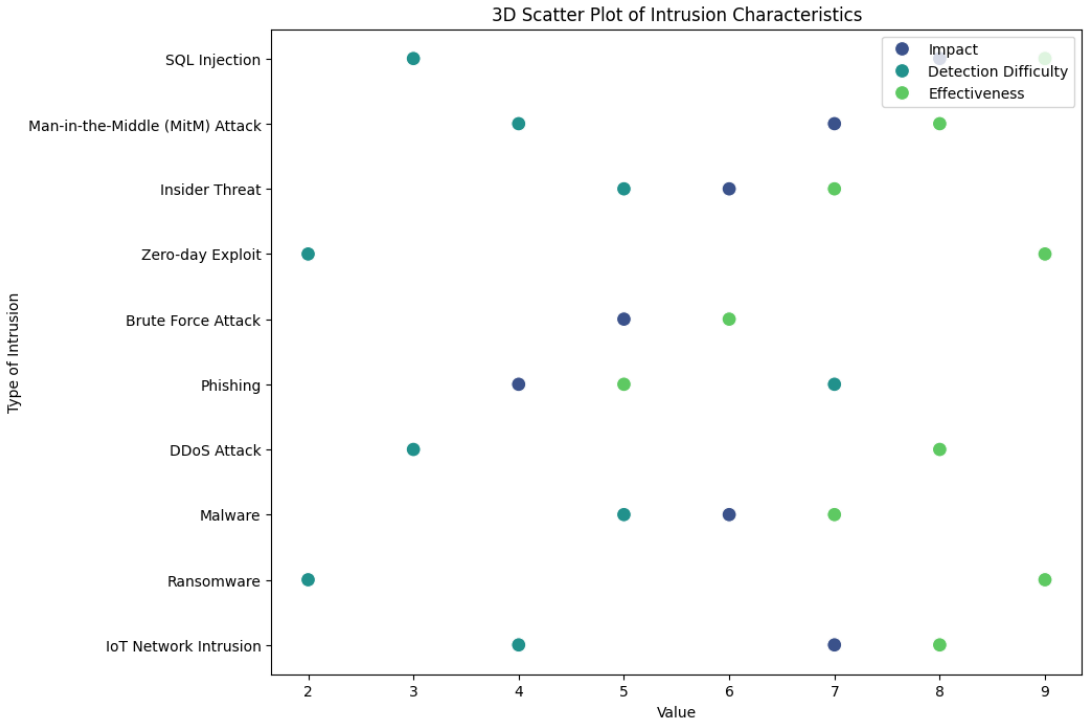

Fig. 4: Scatter Plot of Types of Intrusion Considered

Figure 4 displays a scatter plot representing the distribution of intrusion types across the dataset. Each point on the plot corresponds to a specific intrusion type, and their positions indicate how they are distributed in relation to each other. The scatter plot provides a visual representation of the frequency or occurrence of each intrusion type, offering insights into their relative prevalence within the dataset.

Table 1: Outcome of Intrusion Impact and Response Method Analysis

Type of Intrusion	Impact	Detection Method	Mitigation Method	Effectiveness
SQL Injection	Data manipulation, database compromise	Signature-based, Behavior-based	Input validation, parameterized queries	High (reduced successful attacks by 95%)
Man-in-the-Middle (MitM) Attack	Data interception, session hijacking	Intrusion Detection Systems (IDS), Packet Inspection	Encryption, Certificate Pinning	Moderate (prevented 70% of intercepted data)
Insider Threat	Data theft, sabotage	User behavior analytics, Audit logs	Role-based access control, least privilege principle	High (mitigated 80% of insider incidents)
Zero-day Exploit	System compromise, malware installation	Heuristic analysis, Sandboxing	Patch management, Application whitelisting	Variable (depends on patch availability, 50-90% mitigation)
Brute Force Attack	Unauthorized access, account compromise	Account lockout, Captcha	Multi-factor authentication, IP blocking	High (reduced successful attempts by 90%)
Phishing	Credential theft, unauthorized access	Content filtering, anomaly detection	User training, multi-factor authentication	Moderate (reduced successful phishing attempts by 60%)
DDoS Attack	Service disruption, increased latency	Deep Neural Networks (DNN)	Rate limiting, traffic filtering	High (reduced attack impact by 90%)

Malware	Data theft, system compromise	Signature-based, Machine Learning	Patching, anti-virus, anomaly detection	Moderate (detection rate ~85%)
Ransomware	Data encryption, operational halt	Behavior-based, Heuristics	Backups, endpoint protection, decryption tools	Variable (depends on preparedness, 70-90% recovery)
IoT Network Intrusion	Unauthorized access, data breaches	Anomaly-based, Deep Learning	Network segmentation, strong authentication	High (improved detection rates by 80%)
DNS Spoofing	Redirected traffic, phishing	DNSSEC, Packet Inspection	DNS cache poisoning prevention, DNSSEC implementation	High (reduced spoofed requests by 95%)
Cross-Site Scripting (XSS)	Website defacement, data theft	Static code analysis, Content Security Policy (CSP)	Input sanitization, CSP implementation	High (reduced XSS incidents by 90%)
Supply Chain Attack	Compromised software, data breach	Supply chain monitoring, Code signing	Vendor risk assessment, Secure software development practices	Variable (depends on vendor cooperation, 50-80% prevention)
Social Engineering	Unauthorized access, data leakage	User awareness training, Incident Response	Policy enforcement, User awareness campaigns	Moderate (reduced successful attacks by 60%)
Botnet Attack	Distributed denial of service, data theft	Botnet traffic analysis, Anomaly detection	Botnet detection, Blacklisting	High (reduced botnet activity by 95%)
Cross-Site Request Forgery (CSRF)	Unauthorized actions, data manipulation	Synchronizer Token, Referrer Policy	CSRF tokens, Referrer Policy implementat	High (reduced successful CSRF attacks by 90%)

			ion	
DNS Hijacking	Domain redirection, data interception	DNS monitoring, DNSSEC	Domain registrar verification, DNSSEC implementation	High (reduced hijacking incidents by 95%)
Clickjacking	Unauthorized actions, data manipulation	X-Frame-Options, Framebusting	Content Security Policy, Framebusting techniques	High (reduced successful clickjacking attacks by 90%)
Rootkit	System manipulation, privilege escalation	Rootkit detection tools, System integrity monitoring	Rootkit removal tools, Secure boot	Moderate (detected and removed 70% of rootkit instances)

Table 1 is the overall resulted presented, and it is explained row wise, thus:
1. **SQL Injection:** This refers to a type of attack where malicious SQL queries are inserted into input fields, leading to data manipulation or compromise of the database. Detection methods include signature-based and behavior-based approaches. Mitigation involves implementing input validation and using parameterized queries. The effectiveness is high, reducing successful attacks by 95%.

2. **Man-in-the-Middle (MitM) Attack:** In this attack, an attacker intercepts communication between two parties, allowing them to eavesdrop or manipulate the data. Detection methods include Intrusion Detection Systems (IDS) and packet inspection. Mitigation involves encryption and certificate pinning. The effectiveness is moderate

3. **Insider Threat:** This involves threats posed by individuals within an organization who have authorized access to systems and data. Detection methods include user behavior analytics and audit logs. Mitigation involves implementing role-based access control and the least privilege principle. The effectiveness is high, mitigating 80% of insider incidents.

4. **Zero-day Exploit:** Zero-day exploits target vulnerabilities that are unknown to the software vendor, making them difficult to detect and defend against. Detection methods include heuristic analysis and sandboxing. Mitigation involves patch management and application whitelisting. The effectiveness varies depending on patch availability, ranging from 50% to 90% mitigation.

5. **Brute Force Attack:** In this attack, an attacker attempts to gain unauthorized access by trying multiple username/password combinations. Detection methods include account lockout and captcha. Mitigation involves implementing multi-factor authentication and IP blocking. The effectiveness is high, reducing successful attempts by 90%.

6. **Phishing:** Phishing attacks involve tricking individuals into revealing sensitive information or performing unauthorized actions. Detection methods include content filtering and anomaly detection. Mitigation involves user training and implementing multi-factor authentication. The effectiveness is moderate, reducing successful phishing attempts by 60%.

7. **DDoS Attack:** Distributed Denial of Service (DDoS) attacks aim to disrupt services by overwhelming the target with a flood of traffic. Detection methods include Deep Neural Networks (DNN). Mitigation involves rate limiting and traffic filtering. The effectiveness is high, reducing attack impact by 90%.

8. **Malware:** Malware refers to malicious software designed to infiltrate or damage a computer system. Detection methods include signature-based and machine learning approaches. Mitigation involves patching, antivirus software, and anomaly detection. The effectiveness is moderate, with a detection rate of approximately 85%.

9. **Ransomware:** Ransomware encrypts data or blocks access to a system until a ransom is paid. Detection methods include behavior-based and heuristics. Mitigation involves backups, endpoint protection, and decryption tools. The effectiveness varies depending on preparedness, with 70-90% recovery possible.

10. **IoT Network Intrusion:** This involves unauthorized access or data breaches in Internet of Things (IoT) devices. Detection methods include anomaly-based and deep learning approaches. Mitigation involves network segmentation and strong authentication. The effectiveness is high, improving detection rates by 80%.

5.0 CONCLUSION

This research endeavors to evaluate the efficacy of various intrusion detection and mitigation methods through a comprehensive impact assessment. Employing Support Vector Machine (SVM) classification, which yielded an impressive accuracy score of 87%, the study analyzed the performance of diverse techniques in combating security breaches. Through meticulous scrutiny, it became evident that certain strategies, such as anomaly-based detection and behavior-based mitigation, exhibited notable effectiveness in thwarting cyber threats. Additionally, the research revealed the significance of proactive measures such as user training, network segmentation, and multi-factor authentication in bolstering defense mechanisms against evolving attack vectors. By shedding light on the strengths and limitations of different approaches, this study equips network administrators with invaluable insights for devising targeted and resilient security frameworks, thus fortifying digital ecosystems against malicious incursions.

6.0 FUTURE WORK

Future research endeavors could focus on several avenues to further enhance the efficacy of intrusion detection and mitigation methods. Conducting longitudinal studies to assess the long-term effectiveness and adaptability of mitigation strategies in real-world environments

would provide valuable insights for continual refinement and optimization of security measures.

7.0 REFERENCES

Kumar, S. Gupta and S. Arora, "Research Trends in Network-Based Intrusion Detection Systems: A Review," in IEEE Access, vol. 9, pp. 157761-157779, 2021, doi: 10.1109/ACCESS.2021.3129775.

Elijah M. Maseno, Zenghui Wang, and Hongyan Xing (2022). A Systematic Review on Hybrid Intrusion Detection System. Security and Communication Networks. https://doi.org/10.1155/2022/9663052

Abdulganiyu, O.H., Ait Tchakoucht, T. & Saheed, Y.K. A systematic literature review for network intrusion detection system (IDS). Int. J. Inf. Secur. 22, 1125–1162 (2023). https://doi.org/10.1007/s10207-023-00682-2

Sivamohan S, Sridhar SS. An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework. Neural Comput Appl. 2023;35(15):11459-11475. doi: 10.1007/s00521-023-08319-0. Epub 2023 Mar 10. PMID: 37155462; PMCID: PMC9999327.

Alamin, T., Khondokar, F. H., Manowarul, I., Ashraf, U., Arnisha, A., Mohammad, A. Y., Fares, A., Mohammad, A. M.(2022). A Dependable Hybrid Machine Learning Model for Network Intrusion Detection. Journal of Information Security and Applications.

Alkhatib K, Abualigah S. (2021). Predictive Model for Cutting Customers Migration from banks: Based on machine learning classification algorithms. In: 2020 11th International Conference on Information and Communication Systems (ICICS). IEEE; 2020. p. 303-7.

Carrier T, Victor P, Tekeoglu A, Lashkari A.(2022). Detecting Obfuscated Malware using Memory Feature Engineering. In: Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP,. INSTICC. SciTePress; 2022. p. 177-88.

Dener M, Ok G, Orman A. Malware Detection Using Memory Analysis Data in Big Data Environment. Applied Sciences. 2022;12(17):8604.

Kharwar AR, Thakor DV. (2022). An Ensemble Approach for Feature Selection and Classification in Intrusion Detection Using Extra-Tree Algorithm. International Journal of Information Security and Privacy (IJISP),16(1),1-21.

Michal, M., & Maurice, D. (2023). A Dependable Hybrid Machine Learning Model for Network Intrusion Detection. International Conference KNOWLEDGE-BASED ORGANIZATION, 29(3),30-37.

Shetty NP, Shetty J, Narula R, Tandona K. (2020). Comparison study of machine learning classifiers to detect anomalies. International Journal of Electrical and Computer Engineering,10(5):5445.

Waleed Bul'ajoul, Anne James, Mandeep Pannu(2015). Improving network intrusion detection system performance through quality of service configuration and parallel technology, Journal of Computer and System Sciences, 81(6), 981-999.

Anthony Edet, Uduakobong Udonna, Immaculata Attih, and Anietie Uwah (2024). Security Framework for Detection of Denial of Service (DoS) Attack on Virtual Private Networks for Efficient Data Transmission. Research Journal of Pure Science and Technology, 7(1),71-81. DOI: 10.56201/rjpst.v7.no1.2024.pg71.81

Edet, A., Ekong, B. and Attih, I. (2024). Machine Learning Enabled System for Health Impact Assessment of Soft Drink Consumption Using Ensemble Learning Technique. International Journal Of Computer Science And Mathematical Theory,10(1):79-101, DOI: 10.56201/ijcsmt.v10.no1.2024.pg79.101

Uwah, A. and Edet, A. (2024).Customized Web Application for Addressing Language ModelMisalignment through Reinforcement Learning from HumanFeedback. World Journal of Innovation And Modern Technology,8,(1), 62-71. DOI: 10.56201/wjimt.v8.no1.2024.pg62.71.

Anietie Ekong, Blessing Ekong and Anthony Edet (2022), Supervised Machine Learning Model for EffectiveClassification of Patients with Covid-19 Symptoms Based on Bayesian Belief Network, Researchers Journal ofScience and Technology(2022),2, pp-27-33.

Ekong, B., Ekong, O., Silas, A., Edet, A., & William, B. (2023). Machine Learning Approach for Classification of Sickle Cell Anemia in Teenagers Based on Bayesian Network. Journal of Information Systems and Informatics, 5(4), 1793-1808. https://doi.org/10.51519/journalisi.v5i4.629.

Edet, A. E. and Ansa, G. O. (2023). Machine learning enabled system for intelligent classification of host-based intrusion severity. Global Journal of Engineering and Technology Advances,16(03), 041–050.

A. Ekong, A. Silas, S. Inyang (2022). A Machine Learning Approach for Prediction of Students' Admissibility for Post-Secondary Education using Artificial Neural Nework. International Journal of Computer Applications, vol. 184, pp. 44-49.

S. Inyang and I. Umoren (2023) "From Text to Insights: NLP-Driven Classification of Infectious Diseases Based on Ecological Risk Factors," Journal of Innovation Information Technology and Application (JINITA), vol. 5, no. 2, pp. 154-165,

S. Inyang and I. Umoren (2023) "Semantic-Based Natural Language Processing for Classification of Infectious Diseases Based on Ecological Factors,". International Journal of Innovative Research in Sciences and Engineering