Review

Defending the Digital Frontier: IDPS and the Battle Against Cyber Threat

Hamza Azam , Mohammad Irfan Dulloo , Muhammad Hassan Majeed , Janelle Phang Hui Wan , Lee Tong Xin , Muhammed Ahnaf Tajwar , Siva Raja Sindiramutty *

Posted Date: 9 November 2023

doi: 10.20944/preprints202311.0623.v1

Keywords: Intrusion Prevention System (IPS); Intrusion Detection System (IDS); Intrusion Detection and Presentation System (IDPS); Deep Packet Inspection (DPI); Network-Based Prevention System (NIPS)

Review

Defending the Digital Frontier: IDPS and the Battle Against Cyber Threat

Hamza Azam, Mohammad Irfan Dulloo, Muhammad Hassan Majeed, Janelle Phang Hui Wan, Lee Tong Xin, Muhammed Ahnaf Tajwar and Siva Raja Sindiramutty

Schools of Computer Science Taylor's University Subang Jaya; hamza@sd.taylors.edu.my, mohammadirfan.dulloo@sd.taylors.edu.my, muhammadhassan.majeed@sd.taylors.edu.my, janellehuiwan.phang@sd.taylors.edu.my, tongxin.lee02@sd.taylors.edu.my, mohammedahnaf.tajwar@sd.taylors.edu.my, siva.sindiramutty@taylors.edu.my

Abstract: The ever-evolving landscape of technology continually drives the demand for more robust and secure systems. Intrusion Detection and Prevention Systems (IPS) play a pivotal role in safeguarding digital infrastructures. IPS harnesses a blend of cutting-edge technologies, specifically Network-Based, Wireless-Based, and Host-Based Intrusion Detection Systems (IDS), to fortify network security. This multifaceted approach enhances the system's capacity to scrutinize incoming data and network traffic, effectively reducing the risk of intrusion. In the realm of malicious activity detection, IPS employs a diverse array of techniques and mechanisms. Our proposed IPS integrates both anomaly-based and signature-based analysis approaches. In signature-based analysis, intrusions are identified by matching data collected from various activities with pre-defined signatures, employing rule-based methods to detect anomalies effectively. In the anomaly-based analysis approach, the system juxtaposes current activities with a baseline of normal behaviour to flag any deviations. This is achieved through distance-based methods, ensuring a well-rounded approach to threat detection. Our comprehensive prevention system encompasses a suite of security measures, including anti-virus software, Deep Packet Inspection, and Quarantine. These components work in synergy to detect and thwart malicious activities effectively. Even when concealed or hidden, the IPS remains a reliable sentinel, ensuring the integrity of your digital ecosystem. This review delves into the intricate web of terminologies and concepts surrounding Intrusion Detection and Prevention Systems, shedding light on the evolving technology landscape and the critical role IPS plays in bolstering cybersecurity.

Keywords: Intrusion Prevention System (IPS); Intrusion Detection System (IDS); Intrusion Detection and Presentation System (IDPS); Deep Packet Inspection (DPI); Network-Based Prevention System (NIPS)

1. INTRODUCTION

In recent years, we have witnessed numerous reports of data breaches that have affected thousands of businesses globally. These incidents have had far-reaching implications, impacting customers, business owners, investors, and various other stakeholders. In response to these challenges, security professionals have sought to deploy solutions such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Intrusion Detection and Prevention Systems (IDPS) to address this issue. This paper aims to provide a comprehensive explanation of the issue at hand. Notably, zero-day attacks have made a significant impact in the United States. In 2016, the frequency and intensity of zero-day attacks surged, with over three billion such incidents recorded, as reported in the 2017 Symantec Internet Security Threat Report (Khraisat et al., 2019; Annadurai et al., 2022, Kaur et al., 2022)

A. Definition of IDS, IPS and IDPS

As a vital component of network security, Intrusion Detection Systems (IDS) play the crucial role of detecting and responding to potentially hostile activities and policy violations on networks and systems. IDS solutions come in different forms, including Signature-based and Anomaly-based IDS, each tailored to specific application scenarios. Their respective advantages and disadvantages are summarized in the table below. In the present day, IDS systems and hybrid approaches, which

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 November 2023 doi:10.20944/preprints202311.0623.v1

integrate multiple IDS methods, are gaining increasing popularity and respect within the security community, especially in the context of safeguarding embedded systems (Shurman et al., 2019; Ponnusamy et al., 2022, Sharma, U, et al., 2022, Shafiq, D. A. et al., 2021). The primary objective of an IDS is to swiftly identify various types of malware, a task that a standard firewall may not accomplish. While the IDS may not directly halt an attack, it certainly serves as an early warning system for administrators, enabling them to take other measures to mitigate potential damage (Khraisat et al., 2019. Kumar et al., 2020).

An Intrusion Prevention System (IPS) is defined as a network security system designed to detect and prevent identified attacks from potential attackers (Forcepoint, 2019; Ponnusamy, Humayun, et al., 2022, Humayun, Niazi et al., 2022, Humayun, Almotilag et al., 2022). Essentially, an IPS encompasses all the capabilities of an IDS, having evolved from its predecessor. An IPS continuously monitors a user's network to detect possible malicious activities and gather information on them (Comodo Security Solutions, Inc., 2020; Seong et al., 2021). It promptly reports these findings to the system administrator, facilitating preventive actions such as firewall configuration to thwart future attacks. Another role of an IPS is to enforce corporate security policies and prevent network guests from violating these policies. There are numerous advantages to having an IPS installed on a network. Intrusion Detection and Prevention Systems (IDPS) represent the only fully automated solution for identifying and thwarting network attacks. IDPS combines the capabilities of IDS and IPS to automatically identify and mitigate threats that may exist on the network. This combination ensures network security by allowing IDS and IPS to work hand in hand. The majority of modern IDPS solutions employ hybrid systems and various techniques to ensure security.

Table 1. Comparison between different types of IDS (Shurman et al., 2019).

COMPARISON OF SIGNATURE AND ANOMALY BASED IDS ADVANTAGES AND DISADVANTAGES.

	Signature-based	**Anomaly-based**
Advantages	- Low alarm measure: low false positive rate. - Signature based NID are very precise. - Fast detection period. - Based on well-known DoS attacks patterns.	- Monitors unknown behaviors. - Detects unknown attacks. - Decrease limitations problem.
Weaknesses	- Weak protections against new attacks. - Updated on regular bases before securing a network. - No alarm is set for authorized traffic.	- Produces high false positive rates (captures a lot because behavior based NIDs monitor a system based on their behavior patterns). - Time-consuming in means of doing an exhaustive monitoring due to amount of resources used.

B. Importance of IDPS

Intrusion Detection and Prevention Systems (IDPS) possess several critical features, some of which are highlighted here. Firstly, an IDPS can effectively distinguish between normal and malicious network traffic, thereby safeguarding user privacy (Umich.edu, 2021; Adeyemo et al., 2019). It identifies and terminates malicious traffic being used in attacks. Additionally, IDPS offers multiple threat protection capabilities to thwart brute force password attempts, requiring the

 doi:10.20944/preprints202311.0623.v1

configuration of various security protocols to disrupt such attacks. Furthermore, IDPS can detect fingerprint attempts made by hackers to identify the target system's operating system, a crucial step in potential malicious attacks. At times, IDPS technologies can even modify the content of attacks by removing or replacing malicious components to render them benign. For instance, they can filter out infected files from emails to prevent them from reaching the recipient (VMware, 2021; Ponnusamy, Aun, et al., 2022).

In the larger context, IDPSs are designed to not only detect but also respond to attacks by blocking the intruder. The capability for real-time detection, enabling swift responses, is intricately connected with the system's ability to prevent an attack (Quincozes et al., 2021; Jayakumar et al., 2021).

C. Overview of the proposed solution

In this research paper, the authors aim to design a new Intrusion Prevention System (IPS) to counter modern malicious attacks and intrusion activities. This endeavor involves the development of the IDPS with four primary components: the source of data, the analysis engine, preventive action, and reporting. The research team proposes that the IDPS will encompass three distinct technologies, namely NIPS, HIPS, and WIPS. The integration of these technologies is intended to enhance the overall efficiency of the IPS. Network-based IPS (NIPS) consolidates features from Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and firewalls, forming what is commonly referred to as the Gateway IDS (GIDS). Most NIPS systems utilize both signature-based detection and anomaly-based detection methods (Taylor, 2019). Host-based Intrusion Prevention System (HIPS) functions to monitor the host for any suspicious activities (Safensoft.com, 2020). The implementation of HIPS is essential because it can block malicious actions by hackers and promptly alert users, enabling them to make informed decisions (Din, 2021; Humayun et al., 2021, I. Hussain et al., 2022). HIPS tightly integrates with the operating system and the kernel to monitor and intercept system calls, preventing potential attacks.

Lastly, the IPS incorporates Wireless Intrusion Prevention System (WIPS) technology, designed to enhance the security of wireless networks. WIPS monitors the radio spectrum in the network's airspace for unauthorized access and activities (Just Firewalls, 2020; Zaman et al., 2022). It ensures compliance with standards and regulations, such as the Payment Card Industry Data Security Standard (PCI DSS).

2. COMPONENTS OF IDPS

A. Source of Data

The Intrusion Prevention System (IPS) presented in this paper is a hybrid that incorporates three distinct IDPS technologies: Network-Based, Wireless-Based, and Host-Based. Combining these three technologies results in the collection of diverse data from various sources to enhance the detection capabilities. Below, we will delve into the details of how each of these technologies employed in the proposed IPS acquires and utilizes information.

i. Network-Based

The Network-Based Intrusion Prevention System (NIPS) technology approach enables the proposed IPS to monitor and analyze traffic within a specific network segment and between various systems or devices (Mazhar et al., 2020; Alferidah & Jhanjhi, 2020, Muzamal et al., 2021). NIPS also scrutinizes a wide range of protocols, encompassing network, transport, and application protocols, including TCP/IP layer activities, to detect any signs of malicious or unauthorized activities. Deploying NIPS technology necessitates the use of sensors to gather data, with the number of sensors contingent upon the organization's network size. Fortunately, the addition of new sensors is a straightforward process. The Network Interface Cards (NICs) responsible for monitoring will be placed into promiscuous mode, allowing them to capture all incoming packets, irrespective of their destination IP address or MAC address (Scarfone and Mell, n.d.). In terms of architecture, this IPS proposes an inline approach, which compels network traffic to pass through it. This capability enables it to block traffic, when necessary, akin to a firewall. In some cases, certain sensors may

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 November 2023 doi:10.20944/preprints202311.0623.v1

function as hybrids (Conrad, Misenar, and Feldman, 2017). The architecture is further elucidated in the Figure 1 below.

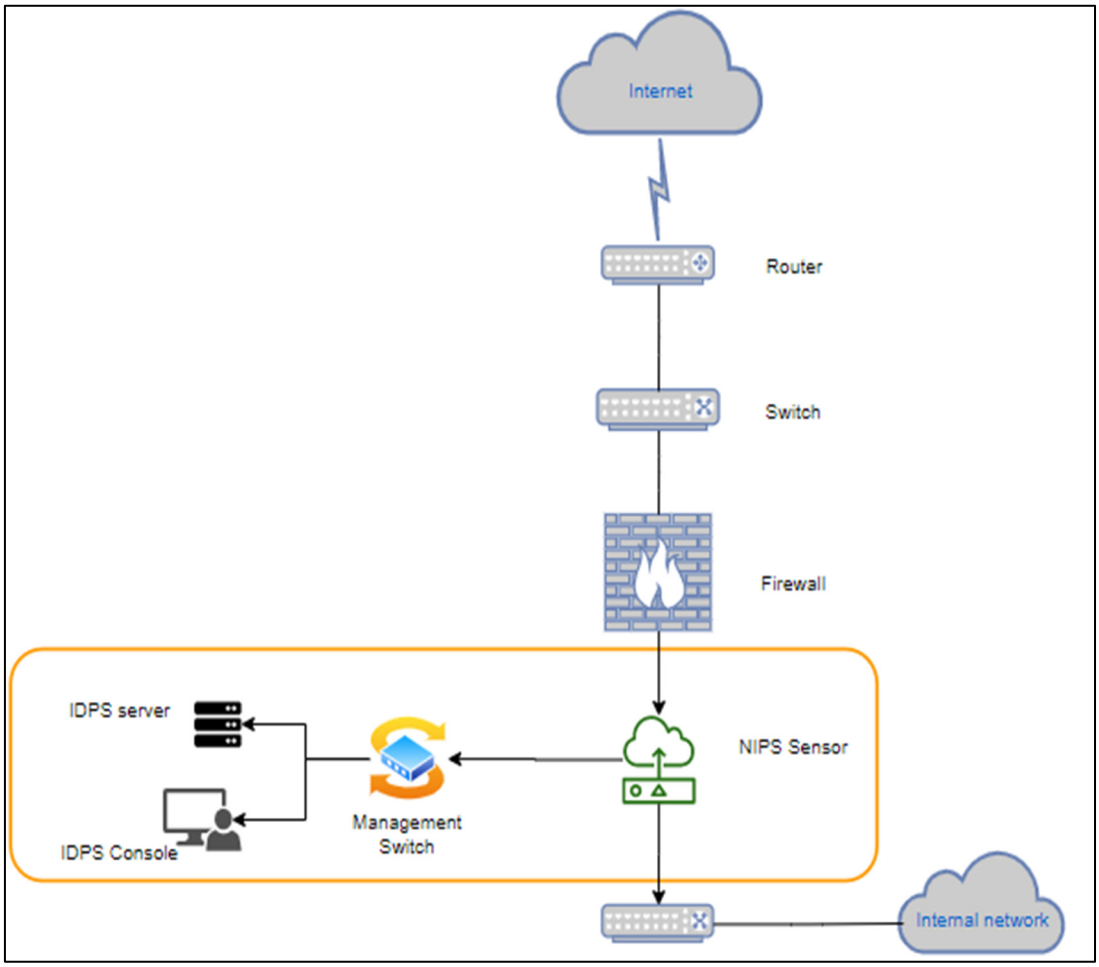

Figure 1. Inline architecture for NIPS.

Data collection capabilities of a NIPS:

A Network-Based Intrusion Prevention System (NIPS) serves as an effective tool for network security. It can detect and categorize network hosts based on IP or MAC addresses, allowing for efficient management and monitoring. Furthermore, the NIPS excels in identifying the operating systems and their respective versions employed by these hosts, a crucial aspect in spotting potential vulnerabilities. It can also pinpoint application versions through port number monitoring and analysis of application-based communications, enhancing threat detection. Moreover, this system's capabilities extend to the identification of network features by capturing and analyzing generic network traffic data, including network device configurations. For example, it can determine the number of hops between devices, enabling the detection of any changes in network configuration.

ii. Wireless based.

The Wireless-Based Intrusion Prevention System (WIPS) technology approach shares similarities with NIPS, as it can be seen as a variant of NIPS, focusing on monitoring wireless network traffic and analyzing wireless protocols to detect any potentially malicious activities conducted on these protocols (GeeksforGeeks, 2019; Ponnusamy et al., 2019). The significance of WIPS in today's context lies in the increasing prevalence of portable devices, with their numbers growing each year. WIPS facilitates the monitoring of wireless local area networks (WLANs) that these portable devices commonly utilize. When deploying the components of a WIPS, they closely resemble those of a NIPS, except for the sensors. In WIPS, wireless sensors are used, and their functionality differs due to the intricate nature of wireless communications. There are two frequency bands to monitor, the 2.4 GHz

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 November 2023 doi:10.20944/preprints202311.0623.v1

and the 5 GHz, both of which are divided into channels to minimize the chances of missing a detection during channel switching. The sensors proposed for this purpose are equipped with robust antennas, enabling them to monitor various channels and cover larger areas (Wireless Intrusion Prevention System (WIPS), n.d; Zaman et al., 2021). The proposed architecture is depicted in the Figure 2 below.

Data collection capabilities of a WIPS:

Typically, a Wireless-Based Intrusion Prevention System (WIPS) is adept at generating and maintaining a comprehensive inventory of Access Points (APs) and Wireless Local Area Network (WLAN) clients, even identifying peer-to-peer ad hoc clients. This roster is constructed using the Service Set Identifier (SSID) and the MAC addresses of the wireless network cards associated with these devices. The sensors integral to the WIPS architecture are highly sophisticated, employing fingerprinting techniques to cross-verify vendor information derived from MAC addresses, even in cases where spoofing is attempted (Samaher Al-Janabi and Ibrahim AlShourbaji, 2017; Zaman et al., 2022a). This list serves a crucial role in creating device profiles for WLAN identification and automatically removing outdated entries. Furthermore, the sensors diligently record the WLANs they encounter, distinguishing them based on their SSID. Network administrators can leverage this information to categorize entries into authorized WLANs, neighbouring WLANs, or potentially rogue WLANs. This data is invaluable for enhancing responses to detected events and facilitates the discovery of new WLANs, thus bolstering the overall security and management of wireless networks.

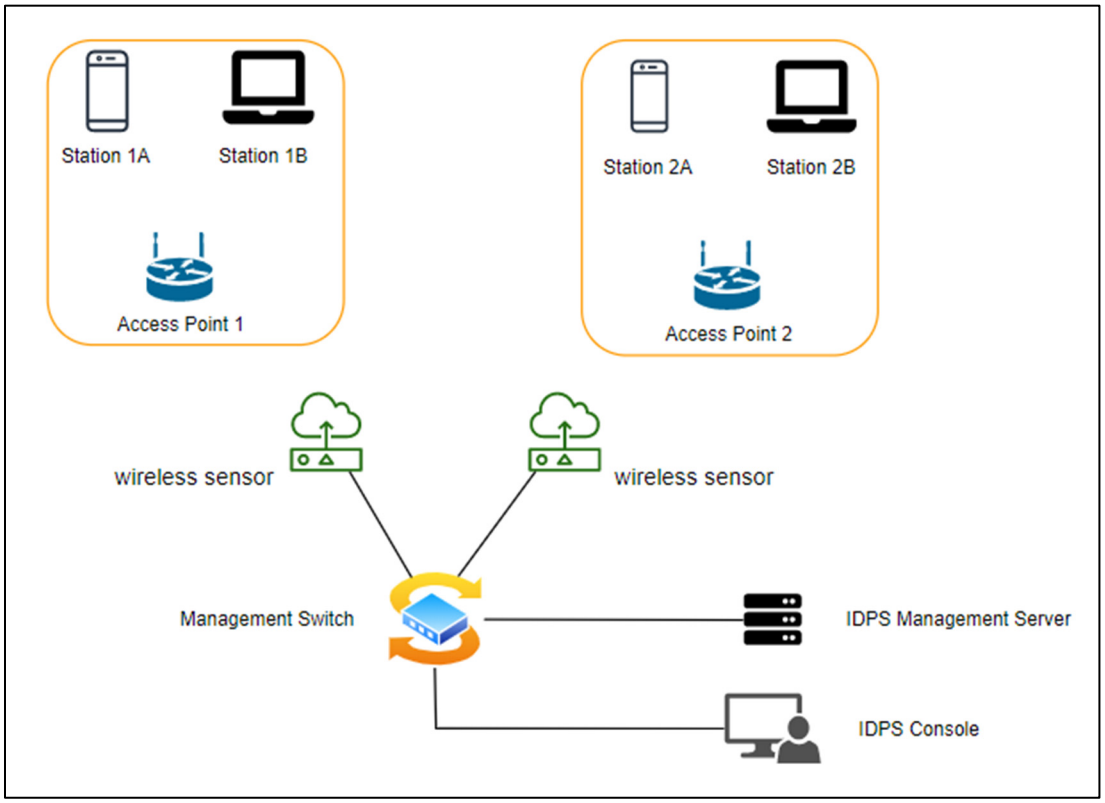

Figure 2. WIPS architecture.

iii. Host-based

A Host-Based Intrusion Prevention System (HIPS) is a technology that primarily focuses on the behavior and events occurring within a single host to detect any suspicious activities within that system. HIPS is primarily designed for intrusion detection and prevention at the application level and operating system level. It has the capability to monitor various aspects, including network activity (both wireless and wired) specific to the host, file access, system logs, and OS version (Certificationkits.com, 2017; Hamid et al., 2019). When it comes to deploying the components of a HIPS, rather than using sensors as proposed for NIPS and WIPS, HIPS employs a software-based

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 November 2023 doi:10.20944/preprints202311.0623.v1

detection system known as an agent. Each agent is responsible for monitoring the activity of a single host, meaning each host will have its own dedicated agent. These agents can be developed to monitor either the server, the client host, or a specific application service. The architecture of the proposed HIPS technology is illustrated in the Figure 3 below.

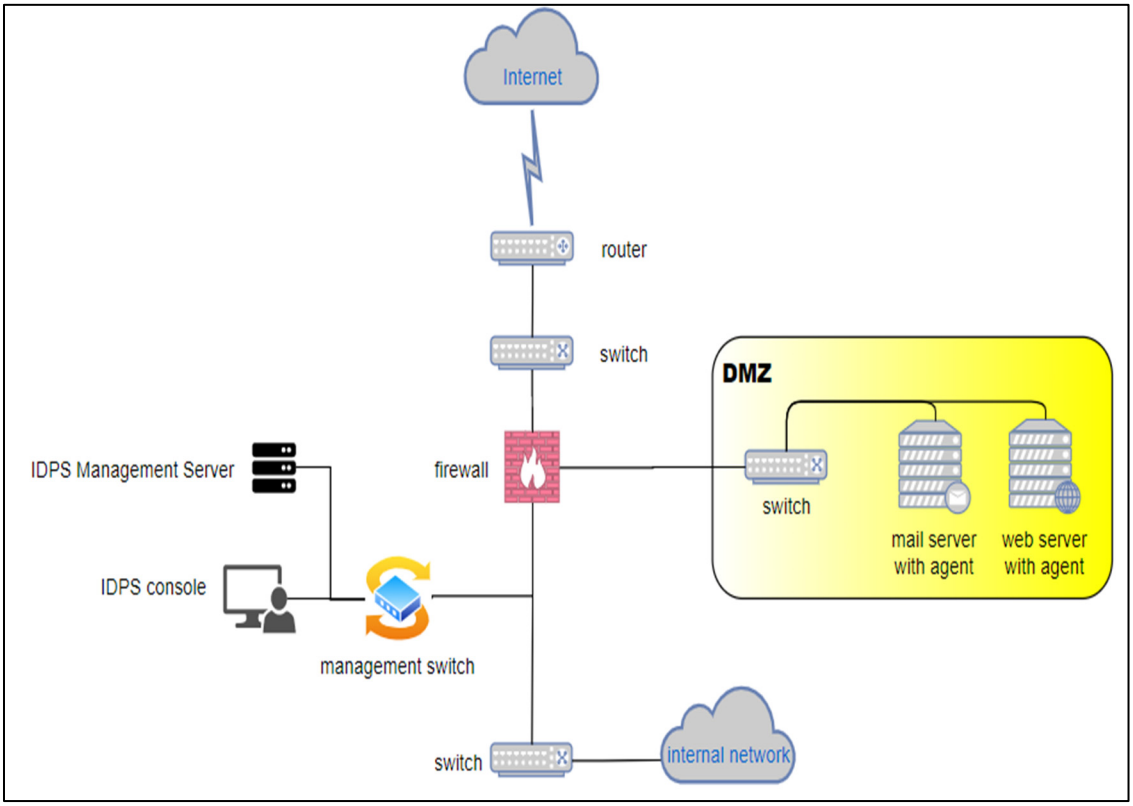

Figure 3. HIPS architecture.

Data collection capabilities of a HIPS:

The kind of data an agent collects solely depends on its detection techniques and what kind of host it is designed to monitor. File systems can be effectively monitored through various techniques, including attribute checking, where agents routinely verify file permissions and access privileges to maintain security and integrity. Another crucial aspect of monitoring involves integrity checking, aimed at detecting any unauthorized alterations to files.

In the realm of application security, agents play a pivotal role by monitoring and analyzing application logs to identify potentially malicious activities. These logs contain critical information, ranging from significant changes in application configuration to failed authentication events, modifications in event logs, adjustments in login information, and more (Sharma et al., 2020; Zahra et al., 2023, Nawaz A et al., 2021, Zahra, F., Jhanjhi, N. Z., Brohi, S. N. et al., 2022). Additionally, agents are proficient at analyzing TCP/IP network packets specific to a host, enabling the identification of suspicious activities such as anomalous sequences of TCP/IP connections occurring within the host where they are deployed. Furthermore, agents possess the capability to scrutinize code using techniques like code behavior analysis. This enables the safe execution of code within a controlled sandbox environment for testing purposes. Agents can also perform vital functions like buffer overflow detection, identifying characteristics of stack and heap buffer overflows by closely monitoring memory segments, thus enhancing overall system security.

 doi:10.20944/preprints202311.0623.v1

iv. Logging capabilities of the proposed IPS

Logging Capabilities of the proposed IPS

Logs play a pivotal role in an IPS as they support the detection and analysis procedures. The specific information generated for logging varies based on the technology in use. While there may be overlaps in some common types of logged data, there can also be information unique to each specific IPS type. Below, we will delve into the logging capabilities of the proposed IPS, encompassing both the common and distinctive data logged by the WIPS, NIPS, and HIPS (Scarfone and Mell, n.d; Vijayalakshmi et al., 2021). Intrusion Prevention Systems (IPS) rely on a range of critical data elements for effective threat detection and response. Timestamps play a crucial role, providing a chronological record of malicious activities or attacks, enabling precise event tracking. Connection ID, also known as session ID, offers a unique identifier for sessions, such as TCP sessions, enhancing the system's ability to monitor and manage network traffic.

A severity rating system, sometimes referred to as impact and confidence, assists in evaluating the seriousness of specific activities or attacks, aiding in prioritizing response efforts. Protocols are essential data points that help identify the type of protocol associated with detected activities, spanning network, application, and transport layers, with common examples including TCP and UDP. Source and destination IP and MAC addresses are instrumental in identifying data flows' origin and destination. Beyond IP addresses, MAC addresses can provide insights into the vendor of a particular system, enriching network monitoring capabilities. Furthermore, IPS systems can scrutinize every byte transmitted or received over a connection, ensuring comprehensive monitoring. Lastly, the countermeasure information pertains to the preventive actions taken by the IPS to thwart intrusion attempts, forming a crucial component of an effective intrusion prevention strategy.

Shelf-life control and data storage

Data storage and the management of data retention are two critical factors that significantly impact the analysis process. In the context of the proposed IPS outlined in this paper, a centralized storage mechanism has been chosen to establish and maintain a central database. This approach allows for the consolidation of all verified and confirmed intrusions classified as true positives into a single logical central database. Such centralization facilitates the correlation of specific attacks or activities across NIPS, WIPS, and HIPS. The central database should possess backup capabilities, such as cloud-based backups or a cloned database, to ensure data security in case of any unforeseen issues affecting the primary database. Equally important is the duration for which data is retained, as it directly influences the efficiency of the IPS and maintenance costs. In the proposed IPS, the data collection points or sensors retain data locally on board for one week, after which it is backed up to the central storage and logging system, where it can be preserved for at least one year. This extended data retention period serves to enhance the analysis capabilities and support reporting within the proposed IPS (Scarfone and Mell, n.d.).

B. Analysis Engine

i. Anomaly detection: Distance-based methods

Distance-based methods are employed for anomaly detection, relying on the calculation of distances between two objects within a geometric representation. In our approach, we utilized a distance-based method implemented through the K-means procedure. The K-means algorithm was employed to train datasets containing both normal and anomalous traffic (Henriques et al., 2020; Almusaylim & Jhanjhi, 2018, Almrezeq, N. et al., 2021, Almusaylim et al., 2020).

We have opted for outlier detection as our preferred method because it excels at identifying anomalies that were not present in the trained datasets. This approach enables the rapid detection of attacks through distance calculations. When an observation deviates from the typical behavior, it's categorized as an outlier. In outlier detection, an object's distance is computed from the center of the normal cluster. If this distance exceeds a predefined threshold, the object is classified as an anomaly or abnormal. In Figure 1, objects with distances exceeding the predefined threshold are considered anomalies (Li et al., 2019; Ubing et al., 2019). We've incorporated the distance-based method into our analysis engine as part of our goal to create an Intrusion Detection System (IDS) with minimal false

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 November 2023 doi:10.20944/preprints202311.0623.v1

alarms. This approach is robust against small variations in patterns and is straightforward to implement and understand. Its ability to detect anomalies with just a few calculations makes it suitable for real-time detection (A review on outlier/anomaly detection in time series data, 2020). The method proposed above is anomaly-based, meaning it can also identify patterns that are not predefined.

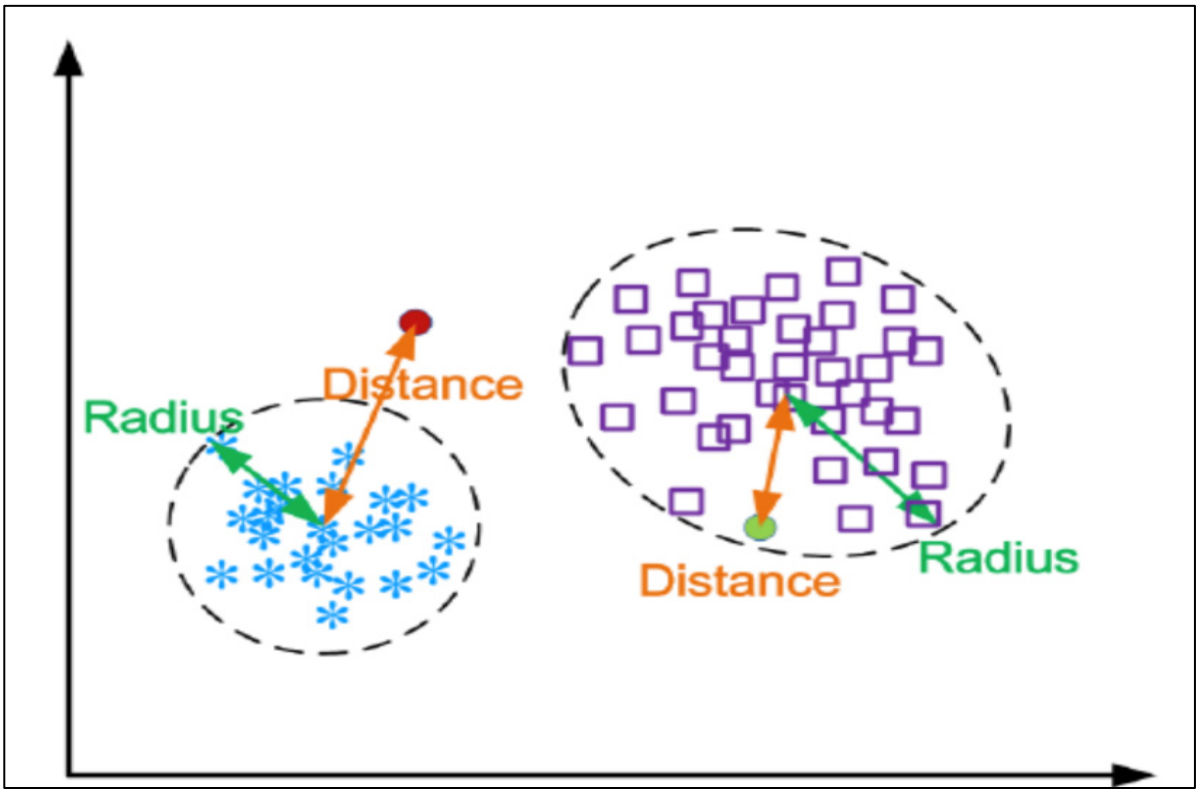

Figure 4. Anomaly Based Detection (Li et al., 2019).

ii. Signature-based detection

In our Intrusion Prevention System (IPS), we have incorporated the Signature-based algorithm as well. This method operates by inspecting, recognizing, and comparing known patterns or signatures within incoming traffic or data packets. A database contains predefined patterns that the algorithm uses to retrieve data for comparison with the current stream of data. These predefined patterns can encompass single events or sequences of events. During the comparison process, if the algorithm detects a matching signature, it triggers an alarm and initiates the appropriate preventive measures (Thapa, Suman & Mailewa, Akalanka, 2020). We have chosen to incorporate the signature-based approach in our analysis engines for several reasons. First and foremost, it minimizes the occurrence of false alarms, reducing both false positives and false negatives. This reduces confusion regarding the prevention mechanism and prevents unnecessary actions, thus avoiding excessive computation. Secondly, the signature-based approach can be highly efficient, especially when the number of signatures is limited. These two factors contribute to preventing system slowdown. Thirdly, the signature-based approach provides precise information about the attacks occurring within the system, thanks to the predefined database. Ultimately, this algorithm operates in a straightforward and user-friendly manner.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 November 2023 doi:10.20944/preprints202311.0623.v1

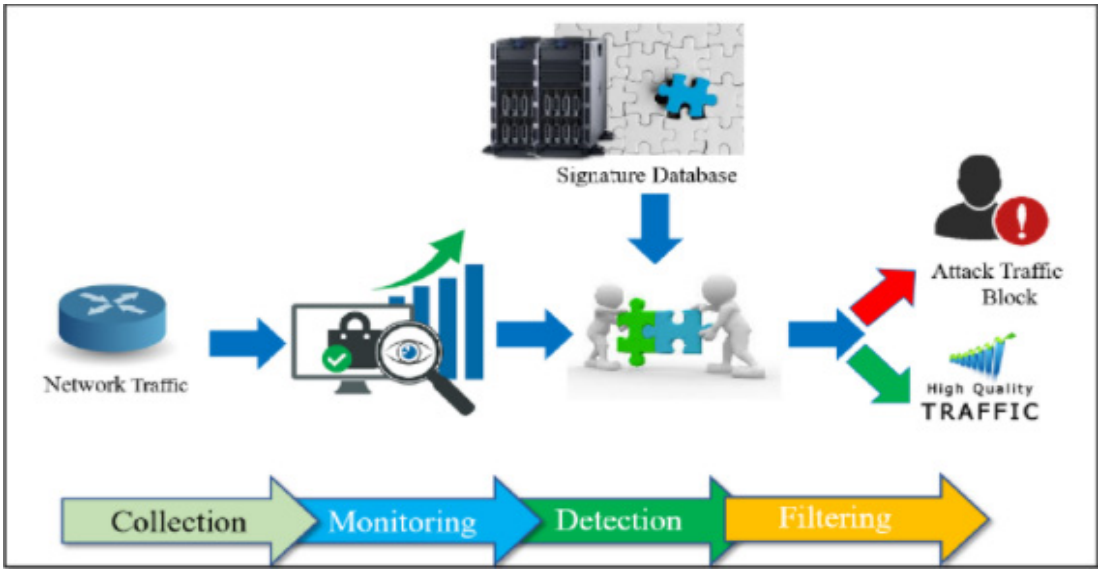

Figure 5. Signature-Based Detection (Hossain Faruk et al., 2021).

iii. Rule-based detection

A rule-based Intrusion Detection System operates by monitoring system events and formulating a set of rules based on these observations. These rules are then used to make decisions about whether a particular pattern of activity is suspicious. Rule-based intrusion detection can be broadly categorized into two techniques: Rule-Based Anomaly Detection and Rule-Based Penetration Identification. While these techniques have their distinct features, there are also instances of overlap between them (Rule-Based Intrusion Detection, 2021; CS406: Rule-Based IDS | Saylor Academy, 2020).

Rule-Based anomaly detection

Rule-based anomaly detection shares similarities with statistical anomaly detection, but it distinguishes itself by generating rules, which is not the case in statistical anomaly detection. In this approach, rules are primarily generated using historical audit records. These records are thoroughly analyzed to identify usage patterns and formulate rules that describe these patterns. The system recognizes past behavior patterns of users, programs, terminals, and other entities. Subsequently, it observes the current behavior to determine if it aligns with the historical behavior patterns. To achieve effectiveness in this type of intrusion detection, a substantial database of rules is essential (Anomaly Detection Rules - TechLibrary - Juniper Networks, 2019)

Rule-Based Penetration Identification

Rule-based penetration detection leverages predefined rules to detect known penetrations or attempts to exploit known vulnerabilities. Additionally, this approach can flag certain system rules as suspicious behavior, even if that behavior falls within established usage patterns. These rules are custom-tailored to the specific machine and operating system. The optimal way to create such rules is through the analysis of attack tools and scripts gathered from online sources.

C. Preventive action

a) Host-based Prevention system.

i. Antivirus

Antivirus software is a critical tool used for detecting, removing, and preventing malicious activities. Once installed on a computer, it operates in the background, offering real-time protection against virus attacks. In addition to safeguarding the computer, antivirus software can also protect files and hardware. It provides supplementary features like website blocking and customizable firewalls (What is Antivirus - Definition, Meaning & Explanation, 2021). Antivirus software can be available in both free and paid versions (What is Antivirus Software, 2021; Saeed et al., 2020, Sangkaran, T. et al., 2020). In our proposed Intrusion Prevention System (IPS), antivirus software will

 doi:10.20944/preprints202311.0623.v1

be installed on the host computer. This antivirus software can eliminate malicious code by scanning computer programs against a database of known attacks. Most modern antivirus programs are designed to update automatically, thereby safeguarding against the latest viruses and attacks (What is an antivirus product? Do I need one?, 2019). Once the IDS (Intrusion Detection System) detects any intrusion, the antivirus software can mark the affected file or program for deletion or render it inaccessible. Furthermore, it can notify the administrator when a virus is detected, enabling prompt action. Regular updates, either manual or automatic, are crucial for antivirus software to protect against the latest threats (Services and (AMP), 2021)

ii. Advanced antivirus

Advanced antivirus solutions have evolved significantly to effectively combat the growing complexity of modern cyber threats. While traditional signature-based antivirus software remains effective at detecting and preventing known malware, it struggles to keep up with the constant emergence of new and sophisticated threats. The introduction of advanced antivirus solutions marks a significant advancement in endpoint security. These solutions harness advanced technologies, including behavioral analysis, artificial intelligence (AI), and machine learning (ML), to identify threats by analyzing malicious intent, rather than solely relying on known malware signatures (Fahad, 2023; Nyunt et al., 2015). Furthermore, advanced antivirus solutions often incorporate EDR (Endpoint Detection and Response), MDR (Managed Detection and Response), and XDR (Extended Detection and Response) capabilities to provide comprehensive protection against evolving cyber threats. Advanced antivirus solutions harness the power of AI and machine learning to significantly enhance threat detection and response capabilities in various areas. Through behavioral analysis and anomaly detection techniques, they can identify deviations from typical behavior, effectively detecting zero-day and unidentified threats. The use of AI-driven classification and predictive analysis improves the ability to categorize threats, even new strains that may share characteristics with known ones, leading to improved accuracy. These solutions enable rapid response to emerging threats by automatic updates, minimizing the risk of compromise (Jacob, 2023).

Endpoint Detection and Response (EDR) plays a vital role in advanced antivirus solutions. EDR software effectively detects and monitors threats in real-time through behavioral analysis, even when specific threat signatures are unavailable. EDR also offers forensic capabilities, facilitating thorough investigations of security events. Additionally, EDR can include automated remediation and threat removal to promptly address potential threats (Fahad, 2023). Managed Detection and Response (MDR) services, as part of advanced antivirus solutions, are increasingly essential in addressing cybersecurity challenges. MDR providers offer a range of cybersecurity tools, including EDR, SIEM (Security Information and Event Management), network traffic analysis, and more, which helps organizations with limited resources or expertise to continuously monitor potential attacks. Extended Detection and Response (XDR) solutions represent the next phase in the evolution of antivirus technology. XDR offers enhanced analysis, intelligent alert suppression, and the ability to identify and correlate threats across various environments, providing a more comprehensive and streamlined approach to threat detection and response (George et al., 2021). Many well-known antivirus companies, including Kaspersky, CrowdStrike, Carbon Black, FireEye, and others, offer EDR, MDR, and XDR solutions to address the evolving cybersecurity landscape.

iii. Quarantine

The Intrusion Prevention System (IPS) will incorporate a robust defense strategy, combining antivirus software with a quarantine capability, and will be configured to thwart backdoor attacks, as outlined by Chen et al. (2018). The operational process is designed as follows:

 doi:10.20944/preprints202311.0623.v1

Upon detecting malware, the IPS will act swiftly, isolating the threat by placing it in the antivirus software's vault to prevent any further damage to the system, in line with Chen et al. (2017). Following this, the antivirus software will initiate a comprehensive system-wide scan to root out any additional threats. If more malware or threats are uncovered, they will also be promptly quarantined, ensuring the system's security. Conversely, if no threats are detected during the scan, the system will be deemed "safe," thus safeguarding it against any further intrusion or potential harm. To ensure that users are kept well-informed about the system's security, the IPS will generate email notifications. These notifications will include an alarm and a detailed summary of recent security events, along with specific information on the steps taken to address them, thereby enhancing transparency and user awareness.

b) Network-Based Prevention System

i. Deep Packet Inspection

Deep Packet Inspection (DPI) is a technique used to meticulously examine the content of data packets as they traverse a monitored network. It's a powerful tool employed in intrusion prevention systems. Unlike standard packet inspection, which typically focuses on header information or destination ports, DPI scrutinizes a broader range of data and the actual content within the packets. DPI is adept at identifying, categorizing, blocking, and redirecting packets that may evade detection by regular packet filtering methods (Brooke, 2018). DPI operates based on specific criteria predefined by authorities. It determines how to handle detected threats, not only identifying them but also tracing their origins through packet content. This enables DPI to recognize threats to applications and services. When DPI identifies malware, it promptly notifies the user, allowing for proactive actions to mitigate potential harm (What Is Deep Packet Inspection (DPI)?, Fortinet, 2021). The implementation of DPI is crucial for bolstering security. Hackers often exploit websites to launch cyber-attacks. DPI can restrict traffic from specific websites, thereby safeguarding the network from potential risks. Moreover, it can uncover malicious packets that may go unnoticed by firewalls or those that are concealed (Chickowski, 2020).

ii. Genetic Algorithm

A genetic algorithm is rooted in biological evolution and natural selection theories, finding applications in artificial intelligence and computer search optimization. Genetic algorithms excel in efficiently exploring vast and unorganized datasets. They are particularly effective in tackling complex problems, whether constrained or unconstrained. Genetic algorithms are commonly employed in machine learning, problem optimization, and various other domains. Optimization seeks to enhance an existing solution by evaluating multiple input sets to derive the best possible result. In the realm of network security, genetic algorithms treat input sets as chromosomes, initially disorganized. They aim to provide the best and most optimal solutions to challenges. For example, this could involve devising a remedy for a detected data breach. To continually learn and improve, the program often incorporates machine learning algorithms and generates mutated offspring over time. These algorithms have valuable applications in the security field, including Intrusion Detection and Prevention Systems (IDPS) (Lambora et al., 2019).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 November 2023 doi:10.20944/preprints202311.0623.v1

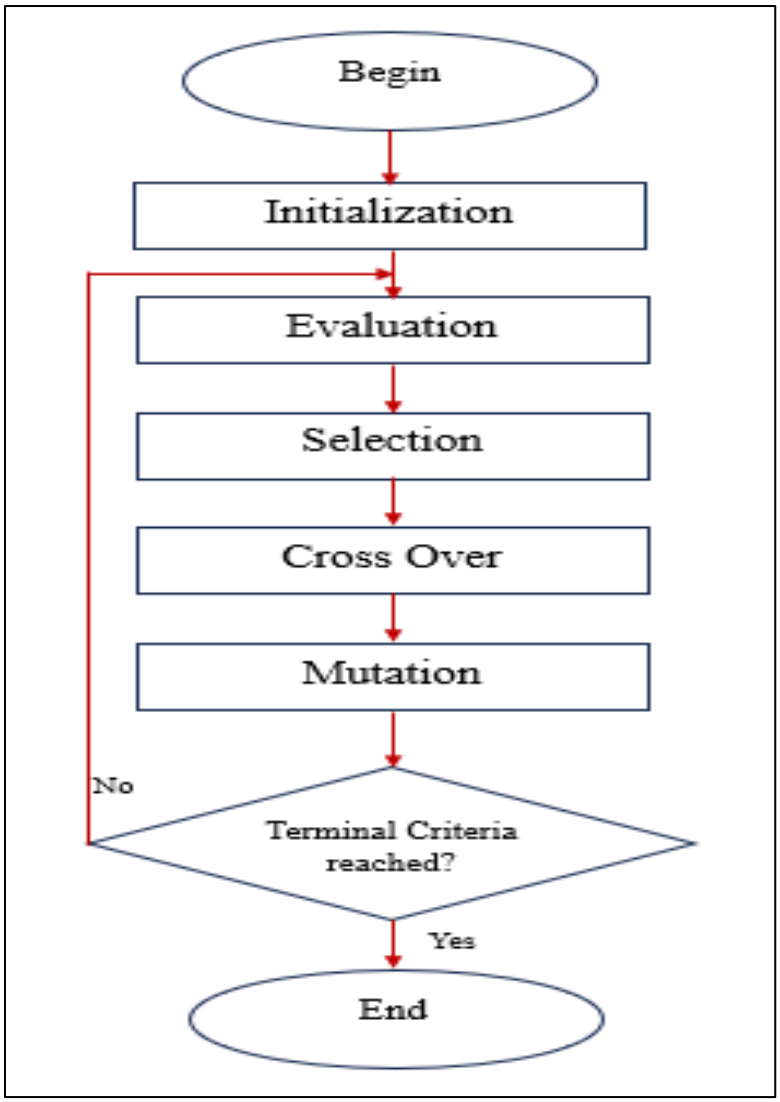

Figure 6. Genetic Algorithm Flow Chart (Lambora et al., 2019).

D. Reporting

i) Information Collected.

To generate reports, the proposed system will collect a substantial amount of information. Within the IDS, two counters will be implemented. The first counter will increment after each intrusion, while the second counter will increase whenever an intrusion is successfully prevented. Additionally, two timers will be employed to track the time it takes to detect and prevent intrusions. The gathered data serves as the basis for generating statistical reports, which play a vital role in enhancing defense against various attacks and threats (Intrusions (IPS) Report, 2021). These reports serve as valuable tools to aid administrators in comprehending the network's vulnerability to different types of attacks. They offer insights into the necessity of additional network devices to fortify the network's security. Furthermore, the reports help pinpoint malicious sources that need attention and highlight suspicious IP addresses, enabling administrators to restrict incoming traffic from these specific sources (IDS/IPS tools - monitoring, 2021)

ii) How to report can improve the defense of the system.

The Intrusion Prevention report offers valuable insights for system enhancement. Information, such as the number of intrusions detected and prevented, holds significant importance for the system.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 November 2023 doi:10.20944/preprints202311.0623.v1

It assists in developing plans and forecasts for improving the prevention system's effectiveness against intrusions. Moreover, it plays a crucial role in enhancing the decision-making process of administrators, enabling them to make informed choices that can prevent further intrusions (IDS/IPS tools - monitoring, 2021).

These reports serve as tools to monitor the progress and development of the intrusion prevention system. They allow for the observation of irregularities and trends, making it easier to diagnose issues effectively. Additionally, the reports act as guiding resources for administrators to thoroughly analyze system vulnerabilities and take proactive measures to address them.

iii) Interpretation of graphs on the reporting

The Intrusion Prevention System (IPS) will include a dedicated reporting and summary section for tracking all activities within a specific timeframe. This graphical user interface (GUI) will enable users to efficiently navigate and utilize the collected data, providing a more visual representation of the system's performance. Consequently, users can assess the effectiveness of the IPS and identify areas that require improvement. This functionality empowers users to make informed decisions and enhance the IPS by pinpointing specific problem areas (Tran et al., 2018).

In Figure 7, we can see a snapshot of the reporting process, focusing on the number of intrusions detected. The graph depicts time on the x-axis and the count of intrusions detected on the y-axis. The initial portion of the graph displays a noticeable increase. This occurs because, upon launching the IPS, it begins detecting some intrusions. However, as time progresses, the system learns and, consequently, detects a greater number of intrusions. Furthermore, over time, we can expect the number of false positives and false negatives to decrease (Khraisat et al., 2019).

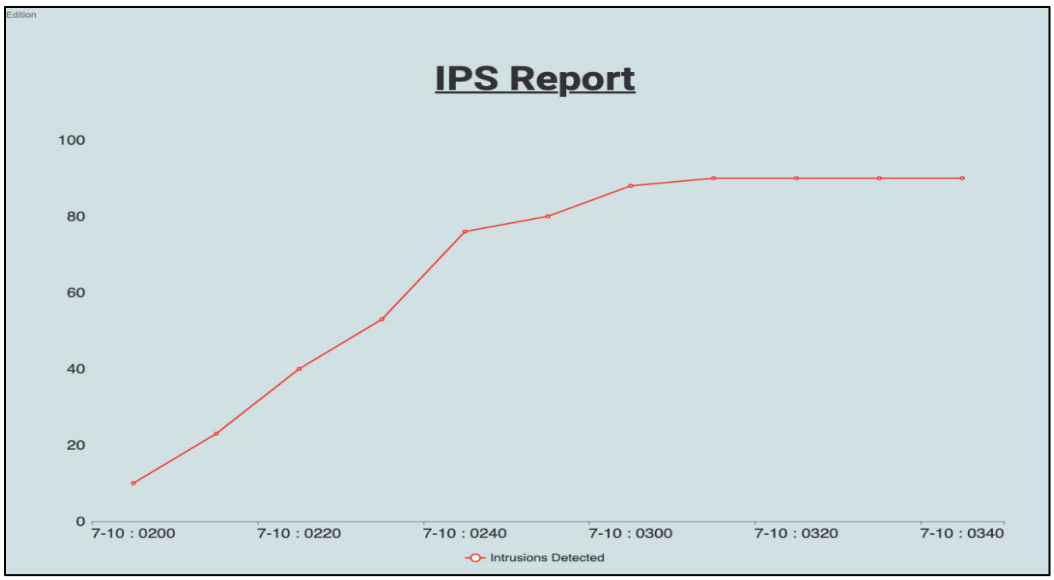

Figure 7. Snapshot of reporting in IDS.

Figure 8 displays a graph where time is plotted on the x-axis, and the number of intrusions prevented is shown on the y-axis. The graph begins with a very low value, indicating that initially, the system detects a minimal number of intrusions. As time progresses and the system undergoes learning and enhancement, it becomes more capable of preventing intrusions. Towards the end of the graph, we observe an upward trend, signifying that the system's performance is improving over time. Consequently, the environment it protects becomes more secure, with the IPS effectively fulfilling its role (Khraisat et al., 2019).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 9 November 2023 doi:10.20944/preprints202311.0623.v1

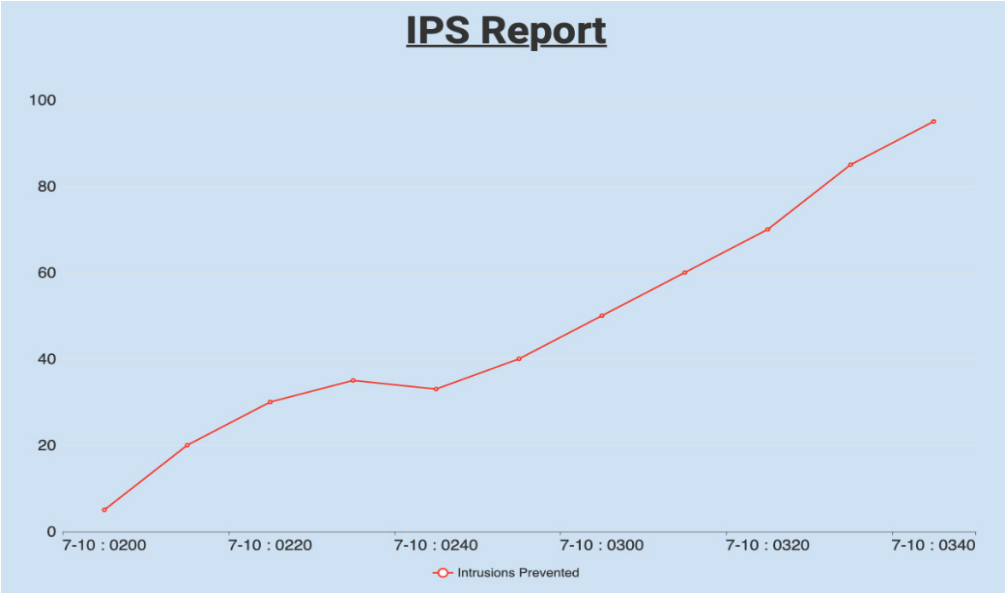

Figure 8. IPS reporting detection.

3. FUTURE PROSPECTS

A. Advancements in IDPS and its potential impact on cybersecurity

As time progresses, Intrusion Detection and Prevention Systems (IDPS) continue to advance in the field of cybersecurity. These systems are increasingly enhancing their effectiveness and efficiency. It's well understood that cybersecurity is a rapidly evolving field that demands constant adjustments to remain pertinent. The following outlines recent and forthcoming developments in IDPS and their significance in the realm of cybersecurity (Prajapati et al., 2021

i. Use of artificial intelligence and machine learning

As we delve further into the AI era, it becomes evident that AI has left a significant imprint on the development of Intrusion Detection and Prevention Systems (IDPS). One notable advantage of this approach is the IDPS's enhanced ability to efficiently identify attacks that exploit zero-day vulnerabilities. As previously mentioned, customary activity profiles can be tailored to the unique requirements of individual systems, applications, and networks. This specificity makes it challenging for attackers to clandestinely carry out actions, as the profiles are customized for each scenario. Furthermore, data gathered through anomaly-based algorithms can be harnessed to create misuse-detecting signatures. Anomaly-based techniques, however, often suffer from the potential for high false-positive rates. This challenge can be mitigated by integrating supervised and unsupervised machine learning algorithms, which can establish an initial baseline and reduce the learning curve of unsupervised machine learning. Hybrid detection approaches incorporate both misuse identification and anomaly detection, resulting in a reduction in false positives for previously undetected cyberattack vectors and an improvement in detection rates for known cyber incursions. This is why many cybersecurity projects based on machine learning and deep learning adopt a hybrid approach (Nunez et al., 2022). Additionally, the utilization of Bayesian algorithms holds considerable importance for approximation models. A Neural Network trained on a Bayesian Classifier can significantly alleviate network traffic burdens for mid to large-sized applications (Nunez et al., 2022).

ii. Cloud-Based IDS

Compared to traditional on-premises Intrusion Detection and Prevention Systems (IDPS), cloud-based IDPS systems offer various advantages, including scalability, flexibility, and ease of deployment. These cloud-based systems, capable of monitoring traffic from different locations, provide a more comprehensive defence against cyberattacks. A study conducted by Abusitta et al. demonstrates their efforts to develop a multi-cloud cooperative cloud IDS integrated with deep

 doi:10.20944/preprints202311.0623.v1

learning algorithms to leverage these advantages, enhancing the usability and effectiveness of incoming IDPS systems (Abusitta et al., 2019).

These innovations are poised to have a significant impact on cybersecurity and the future of IDPS. They promise to improve incident response capabilities, resulting in more effective responses to security incidents. Additionally, they contribute to the enhancement of IDPS detection algorithms, further strengthening the overall security posture.

B. Discussion of potential challenges and solutions

While the advancements in cybersecurity and IDPS systems seem promising, they are not without their challenges. This section will outline some of these challenges and potential solutions. One of the ongoing challenges in the cybersecurity community is the constant evolution of attack types and techniques, with new ones emerging daily. Since IDPS systems are typically trained on datasets that may become outdated within a short timeframe, this poses a significant obstacle to their effectiveness. To address this, experts should focus on researching and training IDPS systems with the latest datasets and emerging attack types to maintain their efficacy (Khraisat & Alazab, 2021).

Another challenge is the complexity of IDPS systems, which can make configuration and administration a daunting task, particularly for organizations with limited IT resources. This complexity is amplified when dealing with Big Data concepts (Faker et al., 2019). One potential solution is the adoption of cloud-based IDS, which offers better manageability and can even be used off-premises. Additionally, organizations can leverage Security Orchestration, Automation, and Response (SOAR) solutions to streamline the management of IDPS systems and other security controls. SOAR technologies automate repetitive tasks, such as alert investigation and crisis management, allowing security personnel to focus on more complex responsibilities like threat analysis and incident handling (Bartwal et al., 2022). This approach enhances the organization's ability to effectively manage IDPS systems.

4. CONCLUSION

This research paper aims to design and propose an Intrusion Prevention System (IPS) capable of preventing highly dangerous and costly intrusion activities. As the organization for which this IPS is intended did not provide specific requirements, the IPS designed in this paper incorporates multiple technologies (data collection sources) and techniques (algorithms) to ensure broader functionality rather than specialization in a single aspect. The proposed hybrid IPS features three distinct detection technologies to maximize its impact across a wide range of devices. Network Intrusion Prevention System (NIPS) safeguards the network by scanning incoming packets. Wireless Intrusion Prevention System (WIPS), essentially a wireless counterpart to NIPS, secures all wireless devices within the organization network, including printers and other office equipment. Host Intrusion Prevention System (HIPS) is implemented to analyze the behavior of individual hosts, such as servers. Each of these data sources generates logs containing crucial information, as discussed in the Data Collection section earlier in this paper.

To manage these logs, a shelf-life control and data storage plan is proposed, utilizing a single logical central database alongside sensor memory that can locally store logs for up to a week before transferring them to the database. These technologies are complemented by state-of-the-art detection algorithms. Anomalies are identified using distance-based methods, such as k-means clustering, which partitions data into non-overlapping clusters. The signature-based approach analyzes incoming traffic by comparing it to known patterns, referred to as signatures. The rule-based approach determines the suspiciousness of an activity based on a set of predefined rules.

In terms of preventive measures, various methods are employed to take action. Anti-virus software is proposed for installation on host computers, capable of detecting malicious code by scanning programs against a database of known attacks. Deep Packet Inspection (DPI) enables an in-depth examination of data packets, facilitating the location, detection, categorization, blocking, and redirection of packets, a task that regular packet filtering cannot perform. In addition to virus scanning capabilities, the anti-virus software includes quarantine features to isolate threats in a vault upon detection. The final step in this process is reporting, which is of paramount importance for the

continuous improvement of the proposed IPS as the volume of collected data increases. Logs, obtained from the data collection section, contain valuable insights that are used to generate reports and visualize threats on a GUI-based dashboard. This dashboard offers analysis and report generation capabilities, along with relevant actions that administrators may need to take. With these components, our proposed Intrusion Prevention System is comprehensive and ready for implementation.

References

Abusitta, A., Bellaiche, M., Dagenais, M., & Halabi, T. (2019b). A deep learning approach for proactive multi-cloud cooperative intrusion detection system. *Future Generation Computer Systems*, *98*, 308–318. https://doi.org/10.1016/j.future.2019.03.043

Adeyemo, V. E., Abdullah, A., Jhanjhi, N. Z., Supramaniam, M., & Balogun, A. O. (2019). Ensemble and Deep-Learning Methods for Two-Class and Multi-Attack Anomaly Intrusion Detection: An Empirical study. *International Journal of Advanced Computer Science and Applications*, *10*(9). https://doi.org/10.14569/ijacsa.2019.0100969

Alferidah, D. K., & Jhanjhi, N. Z. (2020). Cybersecurity Impact over Bigdata and IoT Growth. *2020 International Conference on Computational Intelligence (ICCI)*. https://doi.org/10.1109/icci51257.2020.9247722

Almusaylim, Z. A., & Jhanjhi, N. Z. (2018). A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). *Wireless Networks*, *25*(6), 3193–3204. https://doi.org/10.1007/s11276-018-1712-5

Almrezeq, N. (2021). Cyber security attacks and challenges in Saudi Arabia during COVID-19. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2982-2991.

Almusaylim, A. Z., Jhanjhi, NZ, & Alhumam, A.(2020). Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. Sensors, 20(21), 5997.

Annadurai, C., Nelson, I., Devi, K. N., Ramachandran, M., Jhanjhi, N. Z., Masud, M., & Sheikh, A. M. (2022). Biometric Authentication-Based Intrusion Detection using Artificial intelligence internet of things in smart city. *Energies*, *15*(19), 7430. https://doi.org/10.3390/en15197430

Anomalies Detection and Proactive Defence of Routers Based on Muttiple Information Learning (2019). [online] Available at: <https:/Awww.researchgate.net/publication/334718382_Anomalies_Detection_and_Proactive_Defence_of_Routers_Based_on_Multiple_Information_Learning> [Accessed 12 October 2021].

Arxiv.org. 2020. A review on outlier/anomaly detection in time series data. [online] Available at: <https://arxiv.org/pdf/2002.04236.pdf> [Accessed 12 October 2021].

Bartwal, U., Mukhopadhyay, S., Negi, R., & Shukla, S. (2022). Security orchestration, automation, and response engine for deployment of behavioural honeypots. *2022 IEEE Conference on Dependable and Secure Computing (DSC)*. https://doi.org/10.1109/dsc54232.2022.9888808

Brook, C., 2018. What is Deep Packet Inspection? How It Works, Use Cases for DPI, and More. [online] Digital Guardian. Available at: <https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more> [Accessed 12 October 2021].

Certificationkits.com. (2017). CCNA Security: Network Based vs Host Based Intrusion Detection & Prevention - CertificationKits.com. [online] Available at: https://www.certificationkits.com/cisco-certification/ccna-security-certification- topics/ccna-security-implement-ips-with-sdm/ccna-security-network-based-vs-host-based-intrusion-detection-a-prevention/ [Accessed 18 Oct. 2021].

Chickowski, E., 2020. Deep packet inspection explained. [online] AT&T Business. Available at: <https://cybersecurity.att.com/blogs/security- essentials/what-is-deep-packet-inspection> [Accessed 12 October 2021].

Clements, J. & Lao, Y., 2018. Backdoor attacks on neural network operations. 2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP). Comodo Security Solutions, Inc (2020).

Conrad, E., Misenar, S. and Feldman, J. (2017). Domain 7. Eleventh Hour CISSPID, [online] pp.145-183. Available at: https://www.sciencedirect.comitopics/computer-science/network-based- intrusion-detection-system [Accessed 18 Oct. 2021].

Din, A. (2021). Taking Host Intrusion Prevention System (HIPS) Apart. [online] Heimdal Security Blog. Available at: https://heirndalsecurity.com/blog/taking- host-intrusion-prevention-system-hips-aparu [Accessed 16 Oct. 2021].

Faadooengineers.com. 2021. Rule Based Intrusion Detection. [online] Available at: <http://www.faadooengineers.com/online-study/post/cse/network-management-and-securuty/637/rule-based-intrusion-detection> [Accessed 12 October 2021].

Fahad Ahmed. (2023). The Evolution of Antivirus Software to Face Modern Threats. Security Intelligence. https://securityintelligence.com/posts/antivirus-evolution-to-face-modern-threats/

Forcepoint. (2019). What is an Intrusion Prevention System (IPS)? [online] Available at: https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips [Accessed 16 Oct. 2021].

Fortinet. 2021. What Is Deep Packet Inspection (DPI)? I Fortinet. [online] Available at: <https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection>[Accessed 12 October 2021].

GeeksforGeeks. (2019). Intrusion Prevention System (IPS) - GeeksforGeeks. [online] Available at: https://www.geeksforgeeks.org/intrusion-prevention-system-ips/ (Accessed 18 Oct. 2021].

GEORGE, A. SHAJI., GEORGE, A. S. HOVAN., T. Baskar, & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions -Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.7028219

Hamid, B., Jhanjhi, N. Z., Humayun, M., Khan, A. F., & Alsayat, A. (2019). Cyber Security Issues and Challenges for Smart Cities: A survey. *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*. https://doi.org/10.1109/macs48846.2019.9024768

Hayes, B. (2017). Introduction to intrusion detection and prevention technologies. [online] SearchSecurity. Available at: https://searchsecurity.techtarget.com/tip/Introduction-to-intrusion-detection- and-prevention-technologies [Accessed 16 Oct. 2021].

Henriques, J. et al., 2020. Combining K-means and XGBoost models for anomaly detection using log datasets. MDPI. Available at: <https://www.mdpi.com/2079-9292/9/7/1164/htm> [Accessed October 12, 2021].

Hossain Faruk, M. J., Shahriar, H., Valero, M., Barsha, F. L., Sobhan, S., Khan, M. A., Whitman, M., Cuzzocrea, A., Lo, D., Rahman, A., & Wu, F. (2021). Malware detection and prevention using Artificial Intelligence Techniques. *2021 IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/bigdata52589.2021.9671434

Humayun, M., Jhanjhi, N. Z., Talib, M., Shah, M. H., & Suseendran, G. (2021). Cybersecurity for data science: issues, opportunities, and challenges. In *Lecture notes in networks and systems* (pp. 435–444). https://doi.org/10.1007/978-981-16-3153-5_46

Humayun, M., Niazi, M., Almufareh, M. F., Jhanjhi, N. Z., Mahmood, S., & Alshayeb, M. (2022). Software-as-a-service security challenges and best practices: A multivocal literature review. Applied Sciences, 12(8), 3953.

Humayun, M., Jhanjhi, N. Z., & Almotilag, A. (2022). Real-time security health and privacy monitoring for Saudi highways using cutting-edge technologies. Applied Sciences, 12(4), 2177.

Intrusion Prevention Systems I Benefits of Intrusion Prevention Systems. [online] Comodo. Available at: https:/Iwww.comodo.com/intrusion-prevention-systems.php [Accessed 16 Oct. 2023.

I. Hussain, S. Tahir, M. Humayun, M. F. Almufareh, N. Z. Jhanjhi and F. Qamar, "Health Monitoring System Using Internet of Things (IoT) Sensing for Elderly People," 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2022, pp. 1-5, doi: 10.1109/MACS56771.2022.10023026.

Jacob, D. (2023, July 31). The Role of AI in Enhancing Antivirus Security. Techjockey.com Blog. https://www.techjockey.com/blog/role-of-ai-in-antivirus-security

Jayakumar, P., Brohi, S. N., & Jhanjhi, N. Z. (2021). Artificial Intelligence and Military Applications: Innovations, Cybersecurity Challenges & Open Research Areas. *Preprints*. https://doi.org/10.20944/preprints202108.0047.v1

Juniper.net. 2019. Anomaly Detection Rules - TechLibrary - Juniper Networks. [online] Available at:<https://www.juniperneVdocumentation/en_USIsa7.4.0/jsa-users guide/topics/concept/concept-jsa-user-anomaly-detection-rules.html> [Accessed 12 October 2021].

Just Firewalls. (2020). What is a Wireless Intrusion Prevention System (WIPS)? Wi-Fi Security That's No Longer Up in the Air - Just Firewalls. [online] Available at: https://www.justfirewalls.corriNvhat-is-a-wireless-intrusion-prevention-system/ [Accessed 15 Oct. 2021].

Kaur, M., Singh, A., Verma, S., Kavita, Jhanjhi, N. Z., & Talib, M. N. (2021). FANET: Efficient routing in flying ad hoc networks (FANETs) using firefly algorithm. In Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2021 (pp. 483-490). Springer Singapore.

Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, *4*(1). https://doi.org/10.1186/s42400-021-00077-7

Khraisat, A., Gonda!, I., Vamplew, P. and Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, qalaseta and challenges. Cybersecurity, 2(1).

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, *2*(1). https://doi.org/10.1186/s42400-019-0038-7

Kiourti, P. et al., 2020. Trojdrl: Evaluation of backdoor attacks on Deep Reinforcement Learning. 2020 57th ACM/IEEE Design Automation Conference (DAC).

Kumar, K., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). A Survey of The Design and Security Mechanisms of The Wireless Networks and Mobile Ad-Hoc Networks. In IOP Conference Series: Materials Science and Engineering (Vol. 993, No. 1, p. 012063). IOP Publishing.

Kwon, H. (2020). Detecting backdoor attacks via class difference in deep neural networks. IEEE Access, pp.1-1.

Lambora, A., Gupta, K., & Chopra, K. (2019). Genetic algorithm- A literature review. *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*. https://doi.org/10.1109/comitcon.2019.8862255

Learn About Intrusion Detection and Prevention Staying Open for Business. (n.d.). [online] Available at: https://www.junipernet/documentation/en_US/leam- about/LA_I ntrusion Detectionand Prevention. pdf.

Li, J., Su, J., Chen, R., Wang, X. and Chen, S., 2018. Practical privacy- preserving deep packet inspection outsourcing. Concurrency and Computation: Practice and Experience, 31(22).

Li, T., Ma, J., Shen, Y., & Pei, Q. (2019). Anomalies detection and proactive defence of routers based on multiple information learning. *Entropy*, *21*(8), 734. https://doi.org/10.3390/e21080734

Lies De Kimpe, Michel Walrave, Pieter Verdegem, Koen Ponnet. (2021) What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, Internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology 0:0, pages 1-13.

loulianou, Philokypros, Vasilakis, Vasileios orcid.org/0000-0003-4902-8226, Moscholios, loannis et aL(1 more author) (Accepted: 2018) A Signature-based Intrusion Detection System for the Internet of Things,.. In: Information and Communication Technology Form, 11-13 Jul 2018, (In Press)

Manageengine.com. 2021. IDS/IPS tools - monitoring. [online] Available at: <https://www.manageengine.conVproducts/eventlog/ids-ips-monitoring- reporting.html> [Accessed 12 October 2021].

Mazhar, N., Salleh, R., Asif, M. and Zeeshan, M. (2020). SDN based Intrusion Detection and Prevention Systems using Manufacturer Usage Description: A Survey. International Journal of Advanced Computer Science and

Mohammad Masdari, Hemn Khezri,A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems,Applied Soft Computing, Volume 92,2020,106301,1SSN 1568-4946, https://doi.org/10.1016/j.asoc.2020.106301.

Muzammal, S. M., Murugesan, R. K., & Jhanjhi, N. Z. (2021, March). Introducing mobility metrics in trust-based security of routing protocol for internet of things. In 2021 National Computing Colleges Conference (NCCC) (pp. 1-5). IEEE.

Nawaz, A. (2021). Feature engineering based on hybrid features for malware detection over Android framework. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2856-2864.

N. Sharma, A. Chakrabarti, and V. E. Balas, Eds., Data Management, AONILO and Innovation. Singapore: Springer Singapore, 2020.

Ncsc.gov.uk. 2019. What is an antivirus product? Do I need one?.[online] Available at: <https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product> [Accessed 12 October 2021].

Nunez, Juan E.; Tchegui Donfack, Roger W.; Rohit, Rohit; and Horn, Hayley (2022) "Self-Learning Algorithms for Intrusion Detection and Prevention Systems (IDPS)," *SMU Data Science Review*: Vol. 6: No. 2, Article 20, https://scholar.smu.edu/datasciencereview/vol6/iss2/20

Nyunt, K. S., & Zaman, N. (2015). The Effectiveness of Big Data in Social Networks. In *Advances in data mining and database management book series*. IGI Global. https://doi.org/10.4018/978-1-4666-8505-5.ch018

Online.visual-paradigm.com. 2021. Visual Paradigm Online - Suite of Powerful Tools. [online] Available at: <https://online.visual-paradigm.com> [Accessed 19 October 2021].

Osama Faker and Erdogan Dogdu. 2019. Intrusion Detection Using Big Data and Deep Learning Techniques. In Proceedings of the 2019 ACM Southeast Conference (ACM SE '19). Association for Computing Machinery, New York, NY, USA, 86–93. https://doi.org/10.1145/3299815.3314439

Panagiotou, P. et al., 2021. Host-based intrusion detection using signature-based and AI-driven anomaly detection methods. Information & Security: An International Journal, 50, pp.37-48.

Ponnusamy, V., Aun, Y., Jhanjhi, N. Z., Humayun, M., & Almufareh, M. F. (2022). IoT wireless intrusion detection and network Traffic Analysis. *Computer Systems Science and Engineering*, *40*(3), 865–879. https://doi.org/10.32604/csse.2022.018801

Ponnusamy, V., Aun, Y., Jhanjhi, N. Z., Humayun, M., & Almufareh, M. F. (2022b). IoT wireless intrusion detection and network Traffic Analysis. *Computer Systems Science and Engineering*, *40*(3), 865–879. https://doi.org/10.32604/csse.2022.018801

Ponnusamy, V., Humayun, M., Jhanjhi, N. Z., Aun, Y., & Almufareh, M. F. (2022). Intrusion detection systems in internet of things and mobile Ad-Hoc networks. *Computer Systems Science and Engineering*, *40*(3), 1199–1215. https://doi.org/10.32604/csse.2022.018518

Ponnusamy, V., Rafique, K., & Zaman, N. (2019). *Employing recent technologies for improved digital governance*. IGI Global.

Prajapati, P., Bhatt, B., Zalavadiya, G., Ajwalia, M., & Shah, P. (2021). A review on recent intrusion detection systems and intrusion prevention systems in IOT. *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. https://doi.org/10.1109/confluence51648.2021.9377202

Queen A. Aigbefo, Yvette Blount, Maurido Marrone. (2020) The influence of hardiness and habit on security behaviour intention. Behaviour & Information Technology 0:0, pages 1-20.

Quincozes, S. E., Albuquerque, C., Passos, D., & Mossé, D. (2021). A survey on intrusion detection and Prevention Systems in digital substations. *Computer Networks*, *184*, 107679. https://doi.org/10.1016/j.comnet.2020.107679

Romeo, M.D.S., 2019. An intrusion detection system (IDS) in the internet of things (I0T) devices for Smart Home. International Journal of Psychosocial Rehabilitation, 23(4), pp.1217-1227.

Saeed, S., Zaman, N., Naqvi, M., Humayun, M., & Ahmed, S. (2020). *Ransomware: A Framework for Security Challenges in Internet of Things*. https://doi.org/10.1109/iccis49240.2020.9257660

Sangkaran, T., Abdullah, A., & JhanJhi, N. Z. (2020). Criminal network community detection using graphical analytic methods: A survey. EAI Endorsed Transactions on Energy Web, 7(26), e5-e5.

Safensoft.com. (2020). Host Intrusion Prevention System (HIPS). [online] Available at: http://www.safensoft.com/hips/ [Accessed 16 Oct. 2021].

Saylor Academy. 2020. CS406: Rule-based IDS I Saylor Academy. [online] Available at:

Scarfone, K. and Mell, P. (n.d.). Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) Recommendations of the National Institute of Systems (IDPS) (Draft) Recommendations of the National Institute of Standards and Technology. [online]

SearchSecurity. 2017. What is antivirus software (antivirus program)? - Definition from Whatls.com. [online] Available at <https://searchsecurity.techtarget. com/definition/antivirus-software> [Accessed 19 October 2021].

Seong, T. B., Ponnusamy, V., Jhanjhi, N. Z., Annur, R., & Talib, M. (2021). A comparative analysis on traditional wired datasets and the need for wireless datasets for IoT wireless intrusion detection. *Indonesian Journal of Electrical Engineering and Computer Science*, *22*(2), 1165. https://doi.org/10.11591/ijeecs.v22.i2.pp1165-1176

Services, P. and (AMP), A., 2021. What Is Antivirus Protection?. [online] Cisco. Available at:

Shurman, M. M., Khrais, R. M., & Yateem, A. A. (2019). IOT denial-of-service attack detection and prevention using hybrid ids. *2019 International Arab Conference on Information Technology (ACIT)*. https://doi.org/10.1109/acit47987.2019.8991097

Sharma, U., Nand, P., Chatterjee, J. M., Jain, V., Jhanjhi, N. Z., & Sujatha, R. (Eds.). (2022). Cyber-Physical Systems: Foundations and Techniques. John Wiley & Sons.

Shafiq, D. A., Jhanjhi, N. Z., & Abdullah, A. (2021, March). Machine learning approaches for load balancing in cloud computing services. In 2021 National Computing Colleges Conference (NCCC) (pp. 1-8). IEEE.

Snehi, Jyoti. (2020). Diverse Methods for Signature based Intrusion Detection Schemes Adopted httos://csrc.nist.gov/csrc/media/oublications/so/800-94/rev-1/draft/documents/draft sp800-94-rev1.pdf.

Taylor, C. (2019). Network-Based Intrusion Prevention - CyberHoot. [online] CyberHoot. Available at: https://cyberhoot.com/cybrary/intrusion-prevention/ [Accessed 16 Oct. 2021].

Thapa, Suman & Mailewa, Akalanka. (2020). THE ROLE OF INTRUSION DETECTION/PREVENTION SYSTEMS IN MODERN COMPUTER NETWORKS: A REVIEW...

Tsukermarj E., 2020. What is an intrusion detection system (IDS)= Designing a Machine Learning Intrusion Detection System...

Ubing, A. A., Jasmi, S. Z. A., Abdullah, A., Zaman, N., & Supramaniam, M. (2019). Phishing Website Detection: An Improved Accuracy through Feature Selection and Ensemble Learning. *International Journal of Advanced Computer Science and Applications*, *10*(1). https://doi.org/10.14569/ijacsa.2019.0100133

Umich.edu. (2021). Intrusion Prevention System Benefits / U-M Information and Technology Services. [online] Available at: https://its.umich.edu/enterprise/wifi-networks/network-security/ips/benefits [Accessed 16 Oct. 2021].

Verizon Fios. 2021. What is Antivirus - Definition, Meaning & Explanation. [online] Available at: <https://www.verizon.com/info/definitions/antivirus/> [Accessed 12 October 2021].

Vijayalakshmi, B., Ramar, K., Zaman, N., Verma, S., Kaliappan, M., Vijayalakshmi, K., Vimal, S., Kavita, & Ghosh, U. (2021). An attention-based deep learning model for traffic flow prediction using spatiotemporal features towards sustainable smart city. *International Journal of Communication Systems*, *34*(3). https://doi.org/10.1002/dac.4609

VMware. (2021). Intrusion Prevention System. [online] Available at: https://www.vmware.comttopics/glossary/content/intrusion-prevention-system [Accessed 16 Oct. 2021].

Watchguard.com. 2021. Intrusions (IPS) Report. [online] Available at: <https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/WG-Cloud/Devices/reports/report_intrusiont ips.html> [Accessed 12 October 2021].

Webroot.com. 2021. What is Antivirus Software. [online] Available at: https://www.webroot.com/us/en/resourcesnips-articles/what-is-anti-virus-software [Accessed 12 October 2021].

Wireless Intrusion Prevention System (WIPS). (n.d.). [online] Available at: https://usa.ingrammicro.com/media/Documents/vendors/w/watchguard/tech_brief_wips_081616.pdf [Accessed 18 Oct. 2021].

Zahra, F., Jhanjhi, N., Khan, N. A., Brohi, S. N., Masud, M., & Aljahdali, S. (2022). Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning. *Applied Sciences*, *12*(22), 11598. https://doi.org/10.3390/app122211598

Zahra, F., Jhanjhi, N. Z., Brohi, S. N., Khan, N. A., Masud, M., & AlZain, M. A. (2022). Rank and wormhole attack detection model for RPL-based internet of things using machine learning. Sensors, 22(18), 6765.

Zaman, N., Ahmad, M., Khan, M. S., & Hussain, M. (2022a). The Impact of Cyber Attacks on E-Governance During the COVID-19 Pandemic. In *Advances in electronic government, digital divide, and regional development book series* (pp. 123–140). IGI Global. https://doi.org/10.4018/978-1-7998-9624-1.ch008

Zaman, N., Humayun, M., & Almuayqil, S. (2021). Cyber Security and Privacy Issues in Industrial Internet of Things. *Computer Systems Science and Engineering*, *37*(3), 361–380. https://doi.org/10.32604/csse.2021.015206

Zaman, N., Hussain, K., Abdullah, A. B., Humayun, M., & Tavares, J. M. R. S. (2022). Information Security Handbook. In *CRC Press eBooks*. https://doi.org/10.1201/9780367808228