JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

To Implement IDPS in SDN using Snort

[1]Umer Farooq, [2]Dr. Bhawna Sharma, [3]Er. Sheetal Gandotra

[1]MTech Student, [2]Professor, [3]Associate Professor
[1]Department of Computer Engineering,
[1]Government College of Engineering & Technology Chak Bhalwal, Jammu, India

Abstract: The Intrusion Detection System (IDS) was initially developed to identify potential attacks on specific programs or computers, acting as a vigilant observer within the network. Unlike the more proactive Intrusion Prevention System (IPS), an IDS serves as a watchful sentinel, detecting suspicious activity and alerting administrators without the ability to intervene automatically.

An IPS, on the other hand, takes a more proactive approach by continuously scanning network traffic for potential threats and swiftly taking action to stop any suspicious activity. This could involve notifying the security team, severing dangerous connections, removing offensive content, or initiating further security measures. IPSs, evolved from IDSs, now offer enhanced capabilities, sometimes referred to as "Intrusion Detection and Prevention Systems" (IDPS).

The implementation of an IPS can significantly reduce the workload for security teams and Security Operations Centers (SOCs) by automatically blocking malicious traffic, allowing them to focus on more complex threats. Additionally, IPSs play a crucial role in maintaining network security regulations and aiding compliance efforts, such as meeting standards like the Payment Card Industry Data Security Standard (PCI-DSS) for intrusion detection.

In the realm of software-defined networking architecture, there exists a clear division between control and data forwarding functions. This separation allows for greater flexibility and adaptability in network administration, as control decisions can be made independently of the physical data forwarding processes. However, a drawback of traditional IPS deployment is the fixed duration for blocking malicious activity, regardless of attack frequency.

To address this limitation, the writer proposes the development of an adaptive IPS and IDS utilizing ambiguous logic. This adaptive IPS would analyze the frequency and type of attacks to determine the appropriate duration for blocking attacker hosts. Test results indicate that an SDN network equipped with this adaptive IPS has the capability to detect and block attacks with durations tailored to the specific threat landscape.

In summary, while IDSs serve as essential watchdogs in network security, their passive nature necessitates the use of complementary tools like IPSs and IDSs to actively prevent and mitigate threats. The proposed adaptive IPS presents a promising solution for enhancing network security in the dynamic landscape of cybersecurity.

IndexTerms **- Intrusion Detection System (IDS), SDN, Intrusion Detection and Prevention Systems" (IDPS), Snort, 3 Zero-day Attacks.**

I. INTRODUCTION

All Computer networks are becoming more complex due to the increasing number of electronic devices connected to the network, both on the internet and within the internal network of the organisation. Network administrators will definitely have difficulties managing and carrying out maintenance duties on the network as a result of this. A non-profit organisation called the Open Networking Foundation is creating Software-Defined Networking (SDN), a revolutionary method of network construction, in order to address this problem. Unlike traditional architecture, which combines the data plane and control plane into network devices like switches and routers, SDN divides these components and gathers the control plane in one central area. By centralizing the control plane as the hub of network logic, it simplifies overall network management due to its centralized control and enhanced programmability. [paper 1].

On the other hand, security issues are naturally brought up by the increased complexity of data flow in a computer network and technological breakthroughs. An increase in network traffic also increases the likelihood that attackers may take advantage of vulnerabilities to further their own agendas, as demonstrated by the use of Denial of Service (DoS) attacks. Some malicious attacks are designed to interfere with network services; recent events have shown that these attacks target DNS servers. [Paper -2]

Software Defined Network (SDN) constitutes a foundational framework crafted to disperse a diverse array of traffic throughout the network. SDN integrated with the Internet of Things (IoT) caters to the needs of various applications by monitoring incoming traffic. This achievement is realized through the division of data plane and control plane. The data plane, comprising switches, is constructed with flow tables that facilitate the matching of packets and their subsequent forwarding based on specified actions.[2]

Various strategies exist to address this issue, one option being the implementation of an Intrusion Prevention System (IPS). IPSs have the capability to halt malicious data packets and subsequently prevent access from the originating host of the attack packet. An example of IPS software suitable for deployment on Software-Defined Networking (SDN) is Snort. Using OpenFlow technology, SnortFlow is an Intrusion Prevention System (IPS) tailored for cloud environments. The goal of this system is to improve security in cloud networks by using the programmability of OpenFlow to identify and stop network intrusions. [paper-3]

Indeed, a network fortified solely with a firewall and lacking an Intrusion Detection and Prevention System (IDPS) resembles a high-security penitentiary bereft of patrolling guards. The pivotal importance of IDPS emanates from its dual role in ensuring data protection and privacy within the network infrastructure. This underscores the profound significance of IDPS implementation, as it serves as the vanguard against potential breaches, upholding the integrity and confidentiality of sensitive data traversing digital pathways. [paper-5]

1.IDS/IPS

As a watchful eye on the network, the Intrusion Detection System (IDS) was first created to detect possible attacks on particular applications or computers. An intrusion detection system (IDS) acts as a vigilant sentinel, identifying unusual behaviour and warning administrators without having the ability to take automatic action, in contrast to the more proactive intrusion prevention system (IPS).

In contrast, an intrusion prevention system (IPS) employs a proactive strategy by continuously monitoring network traffic for any security breaches and promptly addressing any questionable activity. This could entail sending word to the security team, cutting off risky connections, deleting objectionable content, or starting additional security procedures. Referred to as "Intrusion Detection and Prevention Systems" (IDPS), IPSs are upgraded security solutions that developed from IDSs.

By automatically blocking malicious traffic, an intrusion prevention system (IPS) can drastically lessen the strain of security teams and Security Operations Centres (SOCs), freeing them up to concentrate on more complicated threats. Furthermore, intrusion prevention systems (IPSs) are essential for upholding network security laws and supporting compliance initiatives, like adhering to intrusion detection requirements like the Payment Card Industry Data Security Standard (PCI-DSS).

There is a distinct separation of control and data forwarding tasks in software-defined networking architecture. Network administrators can now be more flexible and adaptable since control decisions can now be made apart from the actual physical data forwarding procedures. The fixed time of harmful activity blocking, irrespective of assault frequency, is a disadvantage of classic intrusion prevention system deployment.

In conclusion, although intrusion detection systems (IDSs) are crucial for monitoring network security, they are only a passive solution. To actively stop and lessen attacks, you also need to use other tools, such as intrusion prevention systems (IPSs). In the ever-changing field of cybersecurity, the suggested adaptive intrusion prevention system (IPS) offers a viable means of improving network security.

1.1TYPES OF IDPS

The types of IDPS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed.

1.**Network-Based Intrusion Detection and Prevention System (NIPS):** A sort of security system called a Network-Based Intrusion Detection and Prevention System (NIPS) is placed at particular points within a network to keep an eye on all traffic going through it. To find any unusual activity, this system examines network and application protocol activity. NIPS works by comparing behaviour that is seen with a database of known attacks that is usually updated by a security expert. The system stops a known danger from entering the network if it detects activity that matches the threat. NIPS is frequently installed at remote access points, routers, modems, firewalls, and other network boundaries.

There exist two distinct subcategories of Network-Based Intrusion Prevention Systems (NIPS):

A. Wireless Intrusion Prevention Systems (WIPS): The job of monitoring wireless networks is assigned to Wireless Intrusion Prevention Systems (WIPS), which use radio frequency analysis to find unknown devices and rogue access points. These systems are placed in key positions within wireless networks and in areas where unauthorised wireless access could occur.

B. Network Behavior Analysis (NBA): Network Behavior Analysis (NBA) systems scrutinize network traffic to identify irregular patterns of activity. For instance, during a Distributed Denial of Service (DDoS) attack, numerous requests inundate the network, aiming to overwhelm it. While each request may appear legitimate individually, their collective volume indicates a potential threat. NBA systems often complement standard NIPS within an organization's internal networks.

2. Host-Based Intrusion Detection and Prevention Systems (HIPS): Host-Based Intrusion Detection and Prevention Systems (HIPS) are strategically positioned on individual hosts, typically on pivotal servers housing critical data or on public servers serving as gateways to an organization's internal network. Operating as vigilant sentinels, HIPS meticulously scrutinize the flow of traffic within their host systems. These systems are finely tuned to detect and analyze host operating system activities as well as internet protocol suite (TCP/IP) activities. Through their discerning gaze, HIPS serve as the last line of defense, safeguarding the integrity and security of vital digital assets against potential threats and intrusions.

Detection methods Once implemented, an Intrusion Detection and Prevention System (IDPS) employs various techniques to recognize threats. These methods can be broadly categorized into three distinct groups:

Signature-based: Signature-based threat detection involves matching observed activity with a database containing unique patterns or identifiers of previously known threats. While effective against familiar threats, this method may overlook novel threats.

Anomaly-based: Anomaly-based threat detection compares random network activity against a baseline standard. Deviations from this baseline trigger alerts, making it proficient in identifying new threats but prone to generating false positives. The most improved component of IDPS due to advances in machine learning and artificial intelligence is anomaly-based threat identification.

Protocol-based: Protocol-based threat detection functions akin to signature-based detection but relies on predefined organization-specific protocols. Any activity violating these protocols is blocked. However, manual configuration by a security expert is necessary.

An example of an Intrusion Prevention System (IPS) is Snort, a prominent open-source network-based software renowned for its real-time data analysis capabilities using signature-based techniques. Snort exhibits proficiency in mitigating various forms of cyber threats, including denial of service attacks, port scanning, and ARP spoofing. Leveraging signature-based methodologies, Snort operates by employing user-defined rules to discern malicious packets from benign ones. Each rule comprises two components: the rules header, which is further subdivided into smaller sections, and the rules option. Fig. 1 illustrates how Snort works in general [paper -1].

3.SDN FRAMEWORK

Three levels make up a typical SDN architecture: the infrastructure layer, the control layer, and the application layer. The application layer, sometimes referred to as the application plane, offers a number of functions, including system security, traffic control, and job scheduling. Through the Northbound interface (NBI), it transmits its requirements and network information to the control plane. The control plane, which is centred around a conceptual controller, gives SDN applications a comprehensive picture of the system and translates application layer requirements into SDN data pathways. The data layer resources are managed and controlled by these controllers through the use of control logic. The forwarding plane, also known as the data layer, is made up of network elements like switches. These switches follow the controller's instructions to forward network traffic in a simpler manner than traditional switches. The Southbound interface connects the data plane and control plane, enabling programmable management of forwarding operations. Security rules may be more readily modified when the control plane and data plane are kept apart. This facilitates the creation of adaptable networks that can be controlled by software to satisfy particular business needs.

3.1 SDN and OPEN FLOW

Network management is revolutionised by SDN and OpenFlow, which separate the control and data planes. In contrast to conventional configurations, SDN's control plane—which is enabled by a centralised controller—manages network architecture without being part of the data layer. System managers can now dynamically modify communication pathways and eliminate dangerous flow entries thanks to this configuration.

Various controllers drive SDN functionality, each offering unique capabilities:

1.NOX: A C++-based controller, NOX efficiently processes data packets and interfaces with OpenFlow APIs and switches to manage network traffic effectively.

2.POX: This Python-based controller aids in path discovery and network architecture exploration, facilitating efficient network management.

3.FloodLight: Offered by Big Switch Networks, FloodLight acts as a controller, providing instructions to underlying infrastructure on message handling, streamlining network operations.

4.RYU: Another Python-based controller, RYU offers flexibility to developers, supporting custom extensions and protocols such as OpenFlow, NETCONF, and P4, making it ideal for scientific and research applications.

OpenFlow was first designed for cutting-edge research, but it has grown to be an essential part of Software-Defined Networking (SDN), allowing new techniques to be quickly implemented. It makes communication and command exchange between the Control and Data planes smooth and efficient. Network traffic is efficiently managed by the controller through the addition of flow entries to the flow table. Conditions, actions, and statistics that control packet comparison, treatment, and monitoring are included in each flow entry.

To create flow tables on switches, two techniques are used: proactive and reactive. Reactive controllers add packets to the flow table in response to network activity, whereas proactive controllers automatically route incoming packets to connected switches. But OpenFlow's non-standard use of TLS raises security issues, making SDN networks susceptible to rule injection attacks—like Flood attacks—that masquerade as Denial of Service (DOS) attacks.

3.2 Security issues in SDN

The SDN controller stands as a stalwart guardian against potential threats to systems. However, with the surge in customers and network activity, the risk of security vulnerabilities escalates. Particularly concerning is the challenge of detecting limited DDoS attacks with precision while minimizing false positives. Given the pivotal role of the controller in SDN, any malfunction can jeopardize the entire network. Various studies have proposed solutions to address these privacy challenges. One notable drawback is the SDN controller's susceptibility to overload, hindering its ability to process incoming traffic. Enhancing the controller's efficiency necessitates further research. See fig 1 Effectively detecting assaults is difficult because attackers are often changing their strategies to mask harmful communications. By sending an excessive number of mismatched messages to the SDN-switch, the hack seeks to overwhelm network capabilities. SDN security difficulties are further compounded by malware penetration, data manipulation, and denial of service attacks. By faking sources or inundating the controller with messages, a DDoS assault might overwhelm it. Unmatched packets are sent to controllers for review; this means that managing incoming traffic afterward will need human intervention. There is an interruption to the entire system if the incoming traffic surpasses the bandwidth or controller capacity. DDoS attacks in SDN try to compromise system integrity and disrupt network operations by attacking several design planes. Fig. 2, showcases the example of distributed DOS attacks. The subsequent sections depict the potential scenarios of a DDoS attack within an SDN framework across multiple design layers:

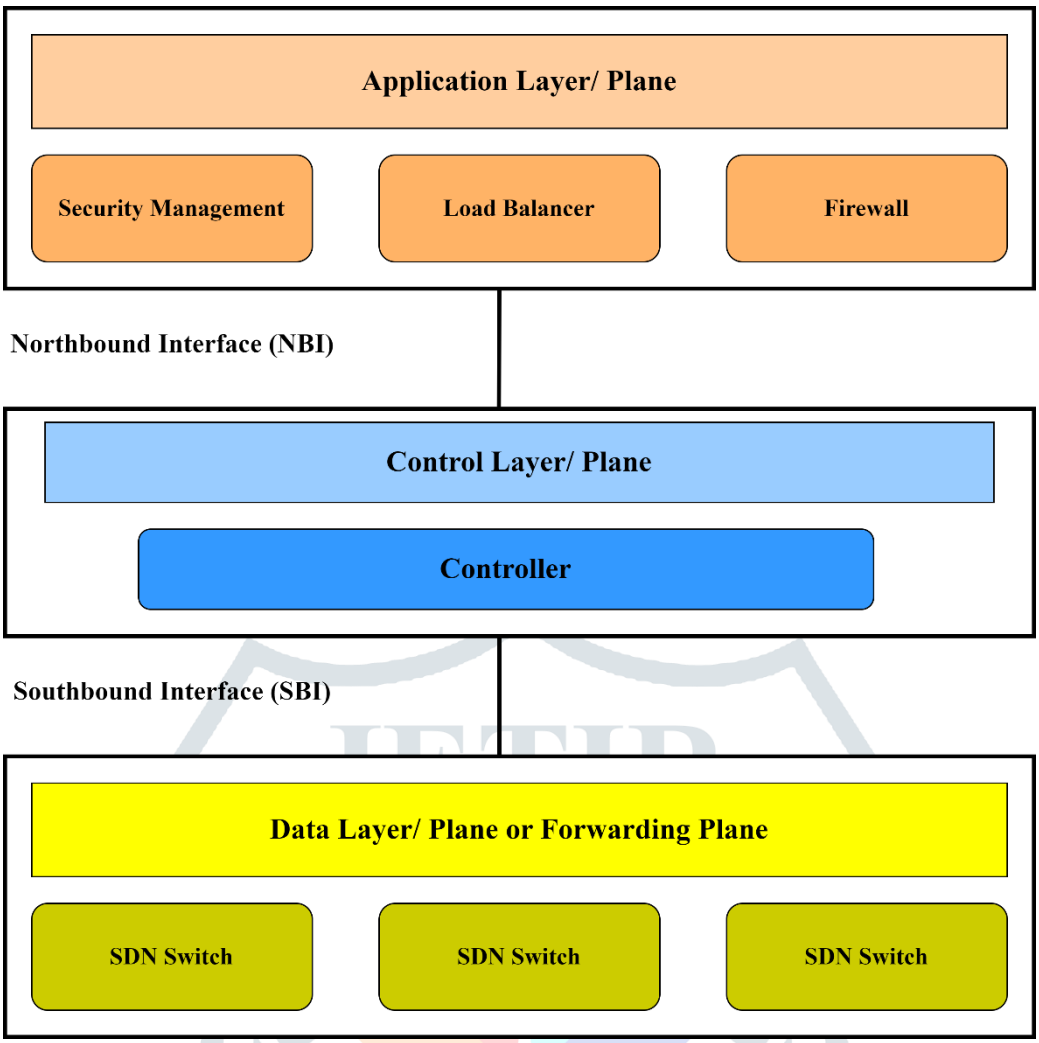

Figure 1 Architecture of SDN

1. Application Layer Assault: In this strategy, the intrusion occurs through malicious applications, monopolizing bandwidth and jeopardizing regular user activities.

2. Control Plane Intrusion: The attacker generates a plethora of requests from fabricated IP addresses, causing the Control Plane to process an excessive volume of Packet in data, leading to delays or denials of legitimate user requests.

3. Interconnectivity Compromise: The intruder targets the network linkage between control and data planes, diminishing overall available bandwidth.

4. Data Plane Exploitation: The assailant overflows the device's flow table, inducing a flow-table overflow attack, disrupting network functionality.

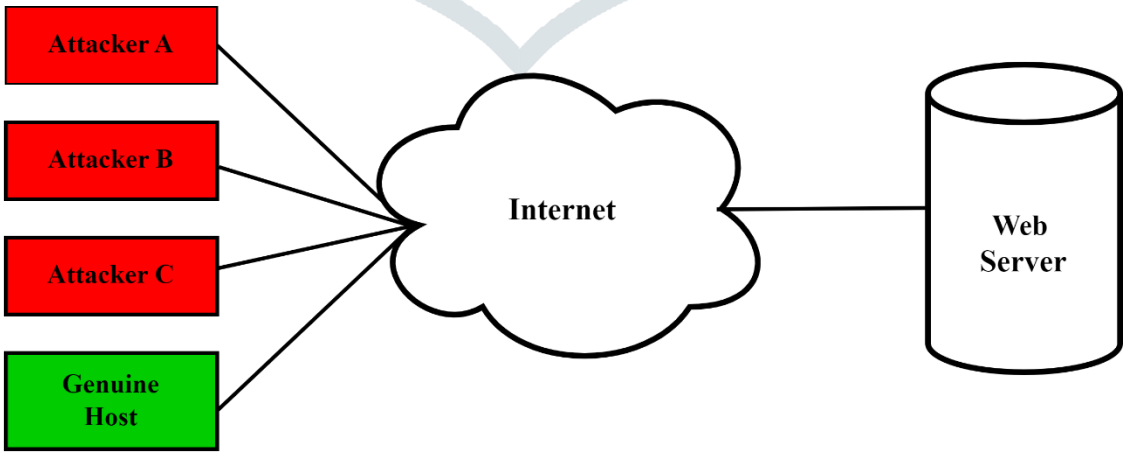

Figure 2 Example of DDOS attack. [10]

3.3 SDN based IDPS

SDN security poses a formidable challenge due to the wide array of SDN implementations available. Therefore, the necessity for an effective Network Intrusion Detection System (NIDS) becomes evident. An Intrusion Detection System (IDS) is a hardware or software solution that actively monitors incoming and outgoing traffic in real-time, analyzing network activity for

potential threats. Upon detection of any malicious behavior, the IDS promptly alerts the network operator and maintains a log of suspicious packet activity. The block diagram depicting the architecture of the Intrusion Detection System within an SDN environment is delineated in Figure 3.

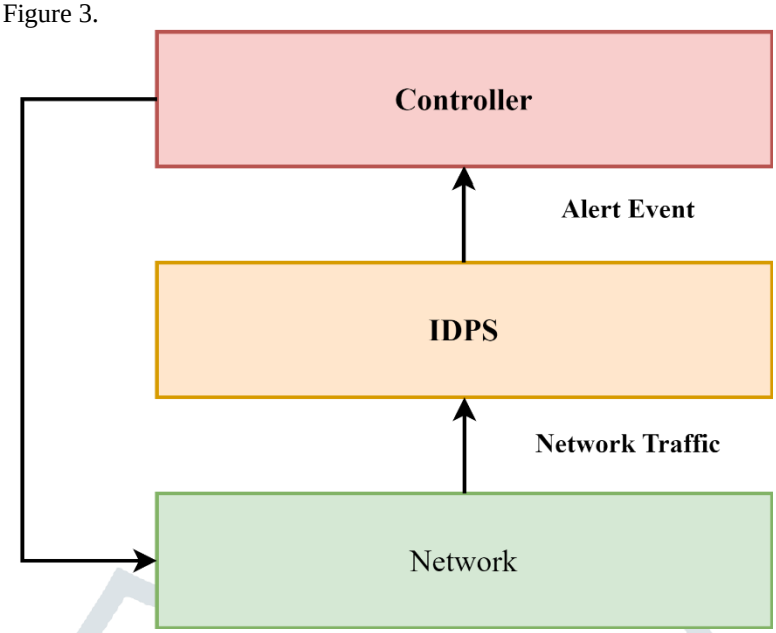

Figure 3. Block diagram of IDS in SDN.

4 Snort

An open-source intrusion detection system called Snort is extensively used by a variety of individuals and organizations. It functions as a signature-based IDPS is well-known for its resilience. Its ability to create unique rules for traffic blocking or alert distribution is what gives it its versatility. Notifications can be easily recorded, shown, or sent by email, providing flexibility in monitoring and reaction. Snort offers a complete network security management solution with a variety of options for rule creation. Snort is structured around four core components: data sniffers, preprocessors, a detection engine, and a log and alarm system. When a packet is captured from the network card, it undergoes initial processing by the preprocessor. Subsequently, the packet is subjected to rule-based analysis in the detection engine. If the packet matches any predefined rules, it undergoes further processing as dictated by those rules. The overarching architecture is depicted in Figure 4.

Because of the possible financial consequences of security breaches, cybersecurity is a major issue for both academic and practical sectors. Key defences include network-based systems (NIDS) and intrusion detection systems (IDS). The two main categories for NIDS detection techniques are signature-based (SNIDS) and anomaly-based (ANIDS). Whereas SNIDS looks for patterns of known threats, ANIDS analyses system behaviour for deviations. SNIDS is good at identifying known dangers, but it has trouble identifying emerging ones. Real-time packet analysis has made Snort, a well-known signature-based intrusion prevention system, famous. Snort is an industry standard for intrusion prevention systems (IPS) because it combines signature, protocol, and anomaly-based techniques. By examining packets, it finds and stops network intrusions.

SNORT is a powerful tool that network administrators use to defend against a variety of cyberattacks, including as buffer overflows, Common Gateway Interface (CGI) intrusions, distributed denial-of-service (DDoS) attacks, and covert port scans. SNORT contains a set of instructions that outline malicious network activity, detects malicious packets, and appropriately warns users of potential threats. SNORT may be downloaded and easily configured, making it suitable for use in both home and office environments. It is compatible with a wide range of operating systems, including Linux, Unix, and the main BSD versions. There are also versions specifically designed for Microsoft Windows settings. Fundamentally, SNORT is supported by the libpcap packet capture package, which makes it possible to examine traffic in real time, archive packets, verify content, and analyse protocols. Libpcap is a highly valuable tool for content parsing, analysis, and TCP/IP traffic interception. It is widely used by astute professionals who want to strengthen their cyber defences.

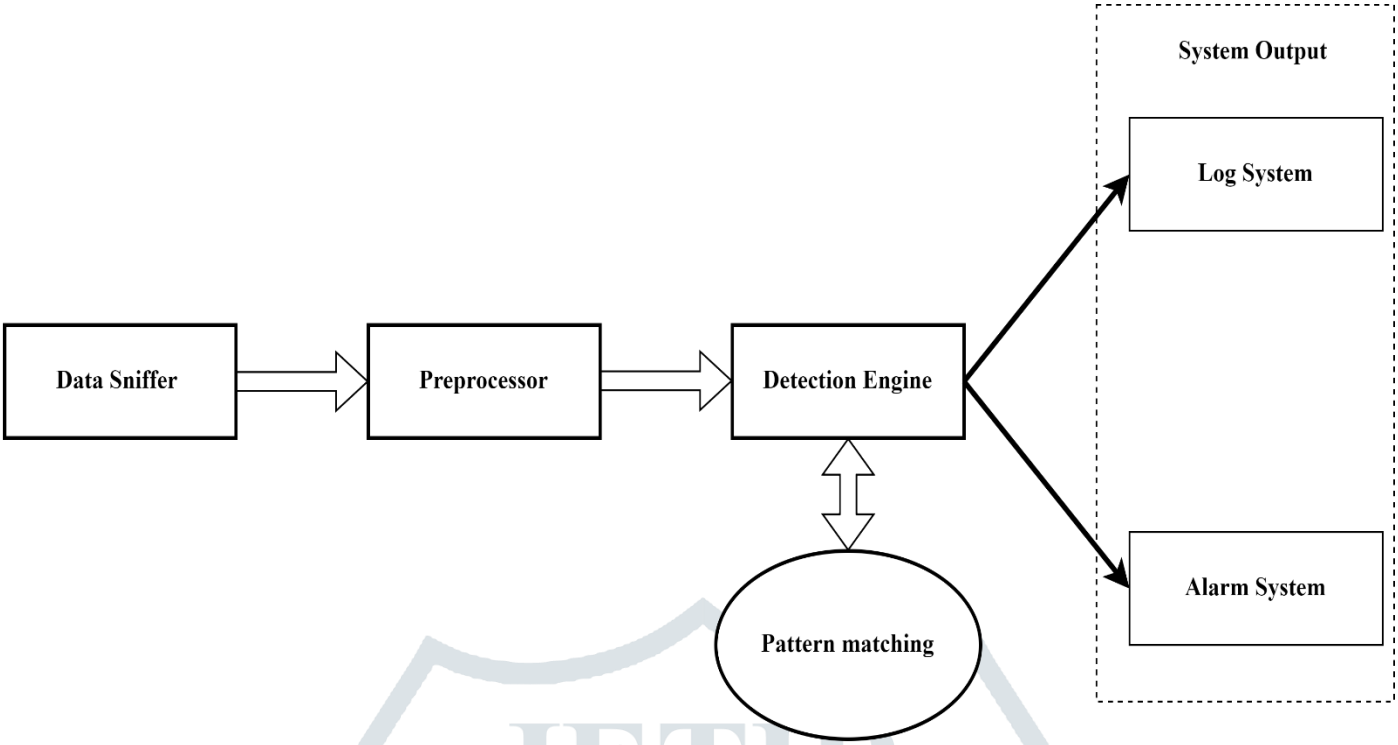

Figure 4 Snort architecture [11]

4.1 Snort Workflow

Snort initialises by processing command line parameters, setting flags, and initialising the PV structure prior to starting its official operations. Subsequently, it creates a linked list of rules by initialising plugins and using predefined rule files. It also initialises the output and preprocessing modules. Using LINPAC structure functions, Snort records packets and processes them appropriately. Packets are processed hierarchically by the network protocol analytic function, which then saves the parsed results in the packet structure. After parsing, Snort looks for intrusions by comparing the output with pre-established rules. If a match is discovered, the output module is used by the system to log the packet or sound an alarm in accordance with the matching rule.

4.2 What is Snort's intended use?

Snort is a prime example of a complex cybersecurity fortress, designed to function in three different ways: It mostly streams network packets continually onto the console when in Sniffer mode, where it passively monitors them. Packets are painstakingly recorded on disc in packet logger mode so they may be examined later. By analysing and scrutinising all network traffic, Snort raises its capabilities to that of a Network Intrusion Prevention Detection System (NIPDS).

A variety of features provide Snort unmatched effectiveness in bolstering network security:

Packet Capturing: To enable thorough packet recording, Snort's packet logger mode painstakingly logs packets to disc.

Live Traffic Tracker: Snort continuously monitors both incoming and outgoing network traffic, providing real-time alerts when it notices any security breaches.

Streamlined Rule Application: The ease of use and flexibility of Snort's rule application procedure allow for quick distinction between malicious and benign network traffic.

Congruence of Content: Snort classifies rules by protocol and port using a multi-pattern matcher, which improves performance especially when identifying potentially dangerous HTTP traffic.

OS Fingerprinting: Snort leverages the distinct TCP/IP stack characteristics of computers to effectively identify the operating system platform utilised by machines that are gaining access.

Broad Applicability: Snort's smooth integration with a variety of operating systems and network configurations guarantees its ubiquitous compatibility.

Cost-free and open-source: Snort is available without charge to organisations, providing them with powerful IDS/IPS capabilities without any financial burden.

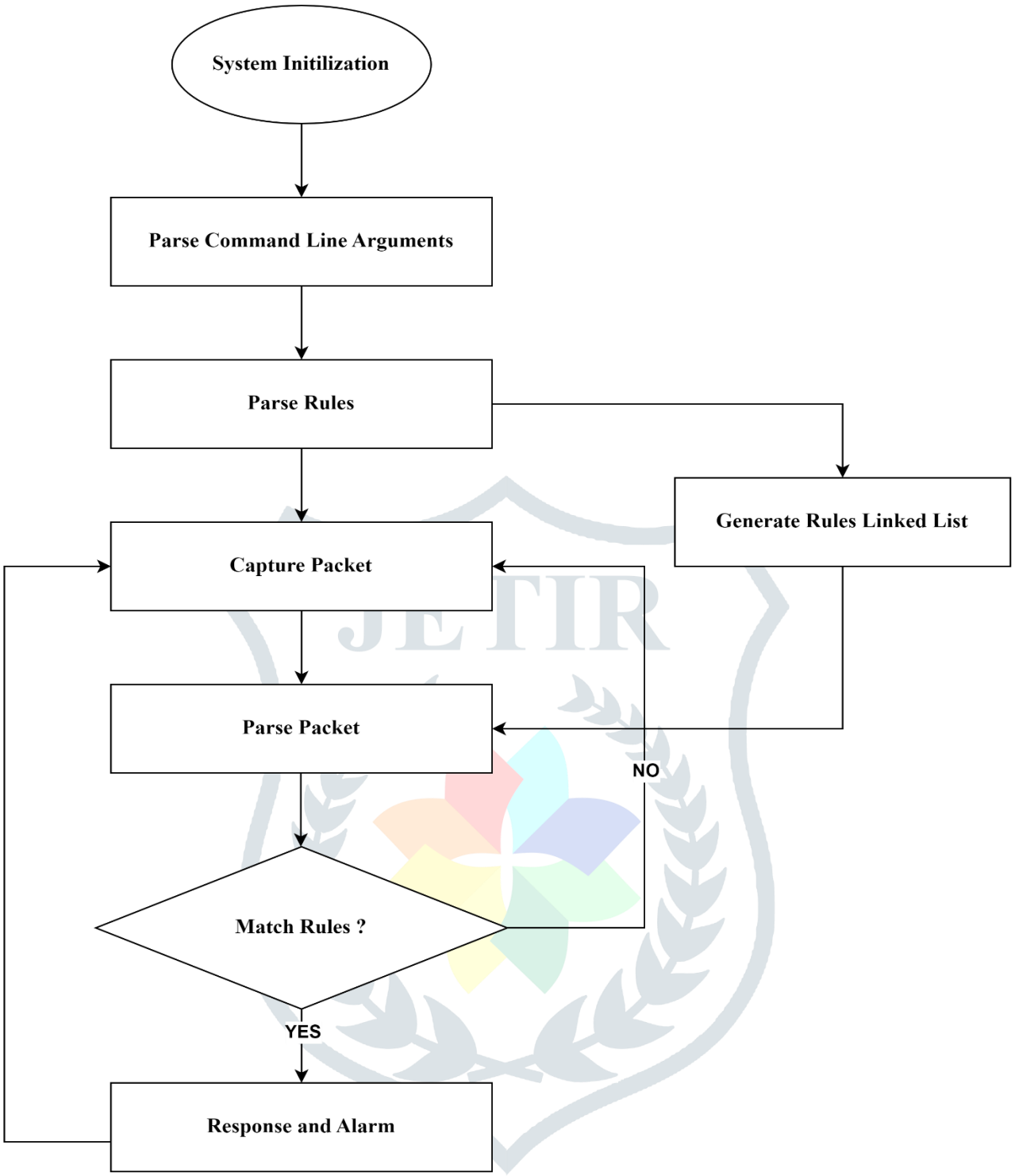

Figure 5 Snort workflow [11]

4.3 Zero-day Attacks and Snort.

A cyberattack that takes advantage of a vulnerability that is unknown to the general public is called a zero-day attack. Since the vulnerability was unknown to the public at the time of the rule set's publication, an attack that targets it after it has been found is regarded by SNIDS (Signature-Based Network Intrusion Detection System) as a zero-day. As an example, CVE-2007-0882 was made public on February 12, 2007. Therefore, unless the SNIDS rule vendor itself found it (and did not report it), which is unlikely, a default SNIDS rule set released before this date cannot incorporate a custom signature for this particular vulnerability. The Snort rule set used in this study was published on November 14, 2006; vulnerabilities discovered after that date are regarded as zero-days for the purpose of the rule set. In order to enable a benchmark test with attacks matching to known vulnerabilities, this rule set was selected to give Metasploit with a significant number of zero-day samples (183 out of 356 assaults) and 173 out of 356 attacks. Consequently, comparing zero-day detection's efficiency to the detection rate of known attacks is essential for proper evaluation.

While Snort may be effective in detecting known threats for which signatures exist, its ability to detect zero-day attacks may be limited. Therefore, it is essential for organizations to complement signature-based IDS like Snort with other security measures, such as anomaly detection and behavior analysis, to enhance their overall threat detection capabilities, particularly for emerging and unknown threats like zero-day attacks [12].

5.LITERATURE REVIEW

In paper [1], Rifqi Fauzan et al. argue that Administrators face issues as a result of the expansion of electronic devices linked to networks, which adds complexity. In response, the Open Networking Foundation developed Software-Defined Networking (SDN), which divides control and data planes for centralised administration. Nonetheless, growing network traffic and developing technology give rise to security issues, as hackers take advantage of weaknesses such as denial-of-service assaults on DNS servers. Although they reduce these hazards, intrusion prevention systems (IPS) like Snort are not flexible enough to respond to different attack frequencies. A fuzzy logic-based adaptive intrusion prevention system (IPS) is one suggested approach. It improves network security and resilience by dynamically modifying block durations in response to assault frequency. The Intrusion Prevention System (IPS) automatically identifies potentially malicious activity within a network. Traditionally, IPS manually scrutinizes anomalous packet data, which is inefficient and resource-intensive. Automating log analysis is recommended for efficiency. IPS relies on two main methods: signature-based and anomaly-based. A. Signature-based IPS compares packets against a database of known malicious attributes but lacks adaptability. B. Anomaly-based IPS compares packets against predefined parameters, triggering alerts for deviations. Snort, an open-source network-based IPS, employs signature-based techniques to analyze real-time data traffic, detecting various attacks. It utilizes user-defined rules to identify malicious packets.

In The academic paper [2] authored by A. Ali et al, "Innovative Three-Tier Intrusion Detection and Prevention System in Software Defined Network," introduces a ground breaking strategy to fortify network security within Software Defined Networks (SDN). The focal point of the study is to bolster security measures in SDN environments through the development of a sophisticated Three-Tier Intrusion Detection and Prevention System (IDPS). The main goal of the project is to apply an enhanced IDPS architecture to improve security protocols in SDN situations. Three tiers make up the proposed system, each of which has a distinct function in strengthening network defense measures. The first layer is devoted to feature extraction, which uses sophisticated methods to identify and examine important characteristics of network data. The next level is intrusion detection, wherein advanced machine learning algorithms—Support Vector Machines (SVM) in particular—are employed to distinguish between benign and malicious activities. Robust packet classification techniques are used in this phase to quickly detect and address possible threats. The last layer of the IDPS architecture is dedicated to intrusion prevention, which uses cutting-edge techniques including packet categorization and Radio Frequency Identification (RFID) to block harmful activities and unauthorised access. Through the integration of various state-of-the-art technologies, the system guarantees all-encompassing defence against a wide range of security weaknesses. Feature extraction, intrusion detection, and intrusion prevention algorithms are important parts of the suggested system. Techniques for feature extraction make it possible to analyse network traffic effectively and extract relevant properties for further study. To precisely identify and classify any security breaches, intrusion detection uses complex machine learning methods, most notably Support Vector Machines (SVM). Techniques for preventing intrusions, such as packet classification and RFID, proactively reduce security risks and preserve network integrity. The study emphasises how important SDN security is, especially in light of new technologies such as the Internet of Things (IoT). Through the integration of sophisticated security protocols that include machine learning algorithms, intrusion prevention methods, and feature extraction, the suggested Three-Tier IDPS provides a strong defence against dynamic cyber threats in SDN environments.

In-depth research on network security is done by Thomas Girdler and Vassilios G. Vassilakis [3], who concentrate on infiltration methods such Address Resolution Protocol (ARP) spoofing. By sending phoney ARP messages and linking their Media Access Control (MAC) address to an authentic device's IP address, adversaries can control network traffic using ARP spoofing. The researchers created an cutting-edge Intrusion Detection and Prevention System (IDPS) based on Software-Defined Networking (SDN) to counter such threats. Their SDN-based IDPS efficiently detects and reduces malicious traffic by dynamically modifying the network's operational settings. The team developed customised IDPS functionality and carried out exhaustive attack tests using specially designed software. A specially created library was used to validate user input and guarantee the resilience of the system, supporting this endeavour. SDN components, such as intrusion prevention systems, firewall capabilities, attack detection, and packet dropping features, have undergone significant improvements. Shorter timeouts were included for quicker mitigation as part of the changes made to speed up response times. The results of their extensive testing indicate that the suggested approach is effective. The detection and mitigation timeframes were found to be very low, usually in a matter of seconds, across multiple test scenarios. This prompt reaction to attempted intrusions demonstrates how well the SDN-based IDPS protects network integrity and thwarts ARP spoofing attacks. the research underscores the importance of proactive measures in combating network infiltration, particularly in the context of ARP spoofing. By leveraging Software-Defined Networking and implementing a robust IDPS, the study presents a viable solution to defend against malicious activities, providing enhanced security for network environments.

T. Xing, D. Huang, L. Xu, C.-J. Chung, and P. Khatkar's paper[4] investigates the creation of SnortFlow, a cutting-edge intrusion prevention system (IPS) designed specifically for cloud environments. Presented at the Second GENI Research and Educational Experiment Workshop in 2013, the study explores the complexities involved in putting SnortFlow into practice within the cloud computing environment. SnortFlow improves network security in cloud infrastructures by utilising OpenFlow technologies. The system achieves a strong intrusion prevention capability by combining OpenFlow-based networking with the popular open-source intrusion detection system, Snort. This combination makes it possible to monitor and mitigate possible risks in cloud systems more effectively. One of SnortFlow's key features is that it can work easily in cloud infrastructures, taking use of the scalability and flexibility that come with cloud computing paradigms. The researchers evaluate the effectiveness of SnortFlow in identifying and preventing malicious activity on cloud servers through a thorough performance assessment. The study emphasises how important proactive intrusion prevention strategies are for defending cloud-based systems against new attacks. Through the integration of OpenFlow technology and Snort's capabilities, SnortFlow provides an advanced solution to tackle the constantly changing security threats associated with cloud computing. An important development in cloud security is represented by SnortFlow, which provides an IPS solution that is customised and makes use of OpenFlow-based networking to improve intrusion prevention capabilities. By bolstering cloud infrastructures against a wide range of potential security threats, the research helps to ensure the integrity and resilience of cloud-based systems against constantly increasing cybersecurity threats.

In paper [5] conducted by Shaghaghi, Arash; Kaafar, Mohamed Ali; and Jha, Sanjay, a novel approach to enhancing network security. The study focuses on devising effective strategies to mitigate various forms of cyber threats and safeguard critical infrastructures against malicious activities. WedgeTail introduces innovative techniques for detecting and preventing cyber attacks, particularly those targeting sensitive networks and communication systems. By leveraging advanced algorithms and analytical methodologies, WedgeTail aims to fortify network defenses and bolster resilience against emerging security threats. Key components of the WedgeTail framework include sophisticated intrusion detection mechanisms, anomaly detection algorithms, and proactive threat mitigation strategies. Through rigorous experimentation and evaluation, the researchers assess the efficacy and performance of WedgeTail in real-world scenarios, demonstrating its effectiveness in identifying and neutralizing potential security breaches. The study underscores the importance of proactive security measures in safeguarding digital assets and infrastructure against evolving cyber threats. By adopting a comprehensive approach to network security, WedgeTail offers a robust defense mechanism capable of adapting to dynamic threat landscapes and mitigating risks effectively. In summary, the research presented by Shaghaghi et al. at ASIA CCS '17 sheds light on the development and implementation of WedgeTail, a pioneering framework for enhancing network security. Through its innovative techniques and proactive strategies, WedgeTail contributes to the ongoing efforts to fortify digital ecosystems and protect against cyber threats in an increasingly interconnected world.

The implementation of an Intrusion Detection and Prevention System (IDPS) using the SNORT framework is examined in the paper[6] "Intrusion Detection Prevention System Using SNORT," written by Tasneem, Aaliya; Kumar, Abhishek; and Sharma, Shabnam. The study explores the role that IDPS plays in defending network infrastructures from cyberattacks and intrusions. The foundation of the suggested system is an open-source programme called SNORT, which is extensively utilised. Its strong skills in network traffic analysis and suspicious activity detection are utilised in this system. Real-time network traffic monitoring, the detection of possible security breaches, and preventive steps to stop unwanted access are important components of the IDPS architecture. By incorporating SNORT, the system uses signature-based detection methods to find known dangerous behaviour patterns, allowing for quick reactions to possible threats. The study also emphasises how crucial it is to update SNORT frequently and modify its rules in order to accommodate changing threat environments. The IDPS maintains its efficacy in identifying and addressing new security threats by customising rules and upgrading its signature database on a regular basis. Extensive experimentation and assessment are used to prove how successful the suggested IDPS solution is at detecting intrusions and preventing unauthorised access to network resources. The research highlights the significance of preemptive security protocols in reducing the potential hazards linked to cyber assaults and guaranteeing the confidentiality and integrity of confidential information. To sum up, the study carried out by Tasneem, Kumar, and Sharma emphasises how important IDPS is for enhancing network security and reducing the risks associated with cyberattacks. The suggested method increases the overall resilience of network infrastructures by providing an efficient defence mechanism against different types of intrusion through the use of SNORT.

The paper [7] titled "Intrusion Detection and Prevention System (IDPS) Technology-Network Behavior Analysis System (NBAS)" by Tiwari Nitin, Rajdeep Solanki Singh, et al, The research highlights the crucial function of NBAS in enhancing IDPS's ability to recognise and avert possible security risks in network settings. An essential part of IDPS, NBAS allows network behaviour patterns to be analysed in order to identify unusual activity that may be a sign of a cyber intrusion. Real-time network traffic monitoring, communication protocol analysis, and abnormal behaviour detection are three of NBAS technology's primary features. NBAS improves the network's overall security posture by using advanced algorithms and machine learning approaches to distinguish between harmful and lawful network events. The report also highlights how crucial it is for NBAS to conduct ongoing monitoring and analysis in order to minimise new security threats and adjust to changing threat environments. NBAS has the ability to recognise and eliminate possible threats before they materialise into serious security issues by utilising proactive surveillance and response systems. Thorough testing and assessment show how useful NBAS technology is in enhancing IDPS's capabilities. Organisations can improve their capacity to identify, stop, and neutralise a variety of cyberthreats and protect vital information by incorporating NBAS into their current security frameworks. The research by Nitin, Singh, Pandya, and others emphasises how crucial NBAS technology is to strengthening IDPS's defences against sophisticated cyberattacks. NBAS ensures the integrity and confidentiality of sensitive data by bolstering the overall resilience and security of network infrastructures with its proactive monitoring and analysis capabilities.

The study conducted by Wassim El-Hajj et al. "On Detecting Port Scanning Using Fuzzy-Based Intrusion Detection System," examines the application of fuzzy logic to improve intrusion detection systems (IDS) for the purpose of detecting port scanning activities. The paper [8] explores the nuances of port scanning, a popular reconnaissance method used by adversaries to identify weak points in target systems' services. Probing network ports to identify possible avenues of entry for illegal access or exploitation is known as port scanning. Due to the clandestine and dynamic nature of port scanning, traditional intrusion detection systems frequently have difficulty identifying it. The researchers suggest a novel strategy that makes use of fuzzy logic inside IDS frameworks to address this problem. A versatile and adaptive method for evaluating network traffic patterns and identifying unusual behaviours suggestive of port scanning efforts is provided by fuzzy logic. Fuzzy logic is a technique that IDS algorithms can use to improve detection capabilities by helping the system discriminate between malicious and benign network activity. The process used to create and verify the fuzzy-based intrusion detection system (IDS) for port scanning detection is described in the study. Experiments carried out on real-world network datasets show that the suggested method is effective in precisely detecting and thwarting port scanning efforts with minimal false positive rates. Furthermore, the study emphasises how crucial proactive defences are in stopping possible cyberthreats like port scanning before they become serious security issues. Fuzzy-based intrusion detection systems (IDSs) can be integrated into network security infrastructures to help organisations protect vital assets and data from sophisticated cyberattacks. In conclusion, El-Hajj et al.'s work provides insightful information about using fuzzy logic to improve intrusion detection systems' capacity to identify port scanning activity. The suggested fuzzy-based intrusion detection system (IDS) shows encouraging results in successfully detecting and thwarting port scanning attempts through rigorous testing and validation, consequently enhancing the general security posture of networked systems.

Paper [9] by Tamara AlMasri, Mohammad Abu Snober, and Qasem Abu Al-Haija, titled "IDPS-SDN-ML: An Intrusion Detection and Prevention System Using Software-Defined Networks and Machine Learning," presents a sophisticated method of improving network security by combining Machine Learning (ML) and Software-Defined Networks (SDN) techniques. In order to successfully detect and mitigate cyber attacks, the study focuses on creating an enhanced Intrusion Detection and Prevention System (IDPS) that makes advantage of the programmable nature of SDNs and the predictive capabilities of ML algorithms. Through the utilisation of SDN architectures' centralised control and dynamic reconfiguration features, the suggested IDPS can effectively monitor network traffic, identify trends, and react to security problems instantly. Moreover, the IDPS can now learn from past data, recognise unusual activity, and update security policies in real time to proactively address new threats thanks to the integration of ML algorithms. The IDPS-SDN-ML system can be made more accurate and effective at identifying and stopping a variety of cyberattacks, such as denial-of-service (DoS) attacks, malware infections, and intrusion attempts, by means of ongoing learning and improvement. The study emphasises the significance of taking a comprehensive strategy to network security, noting that companies may become more resilient against changing cyberattacks by combining SDN and ML technologies. The proposed IDPS-SDN-ML system provides a strong defence mechanism to protect important assets and data in contemporary network settings by fusing the agility of SDN-based network management with the predictive powers of ML-based intrusion detection. In conclusion, by using the synergies between SDN and ML technologies, AlMasri et al.'s research offers a fresh paradigm for developing an advanced IDPS. Empirical validation and testing show that the proposed IDPS-SDN-ML system successfully mitigates cyber threats and improves network security posture, showing promising outcomes.

A novel method for improving network security in Software Defined Networking (SDN) environments is presented in the research paper [10] titled "Network Intrusion Detection in Software Defined Networking with Self-Organized Constraint-Based Intelligent Learning Framework," written by Anurag Bhardwaj et al. The paper offers a unique framework for creating a reliable network intrusion detection system (NIDS) that is suited for SDN architectures by fusing intelligent learning techniques with the concepts of self-organization. Through the utilisation of SDN's programmable features and centralised control, the suggested architecture allows for dynamic adjustment in response to changing network circumstances and cyber threats. Advanced learning algorithms that examine network traffic patterns and identify abnormalities suggestive of intrusion attempts are crucial elements of the architecture. Because of the framework's self-organizing characteristics, autonomous adaptation and optimisation are made easier, enabling the NIDS to constantly learn and increase the accuracy of its detections over time. Furthermore, by adding constraints and domain-specific knowledge to the learning process, the use of constraint-based learning techniques improves intrusion detection precision. This reduces false positives and false negatives by improving the NIDS's ability to distinguish between benign and malicious network activity. The study emphasises how critical it is to implement clever and flexible methods for network security, especially in complex and dynamic SDN systems. Through the integration of constraint-based learning and self-organization principles, the suggested architecture provides an effective and proactive way to identify and address network breaches, improving overall security posture. In conclusion, Bhardwaj et al.'s paper offers a comprehensive framework that uses intelligent learning and self-organization to identify network intrusions in SDN settings. By means of empirical assessment and testing, the suggested framework exhibits encouraging outcomes in proficiently detecting and alleviating cyber hazards, so promoting the progress of network security in SDN implementations.

Ruinan Chi's work [11], "Intrusion Detection System Based on Snort," presents a comprehensive method of intrusion detection that makes use of the Snort system. The suggested intrusion detection and prevention system design is based on the well-known open-source intrusion detection and prevention system Snort. The system analyses network traffic and detects possible security risks using signature-based approaches. The intrusion detection system (IDS) can efficiently monitor network traffic, identify suspicious patterns, and provide real-time warnings by using Snort's capabilities. The system's capacity to stop malicious actions is improved by the vast coverage of known attack signatures made possible by the use of Snort's rule set. Furthermore, to further enhance Snort's detection capabilities, the IDS architecture incorporates cutting-edge algorithms and approaches. This involves using machine learning algorithms and anomaly detection techniques to find new and undiscovered dangers. The configuration of rules, deployment techniques, and performance assessment measures are all covered in detail in this article, which offers insights into the design and implementation of the Snort-based intrusion detection system. The efficiency and efficacy of the IDS in identifying and resolving intrusions are evaluated empirically, underscoring its potential as a useful instrument for network security. All things considered, Chi's study emphasises how important it is to use proven intrusion detection systems, such as Snort, to create reliable and efficient security solutions. Through the integration of sophisticated algorithms with Snort's signature-based detection, the suggested intrusion detection system provides a holistic strategy for protecting network infrastructure from constantly changing cyber threats. conclusion In conclusion, the integration of Intrusion Detection and Prevention Systems (IDPS) within Software-Defined Networking (SDN) architectures presents a robust approach to network security. While traditional IDPS tools such as Snort offer signature-based detection, the proposed adaptive IPS enhances security by dynamically adjusting block durations based on attack frequency. SDN's separation of control and data planes allows for greater flexibility and adaptability in network management, albeit with security challenges such as DDoS attacks. Despite these challenges, advancements in SDN frameworks and IDPS technologies offer promising solutions to safeguard network integrity and mitigate evolving cyber threats.

The paper [12] main focus is on examining how well signature-based intrusion detection systems (IDS) identify zero-day attacks, or cyberattacks that take use of vulnerabilities that are not widely known to the public. The author aims to clarify if conventional intrusion detection systems (IDS), which depend on pre-established patterns or fingerprints of well-known assaults, has the necessary capabilities to detect and neutralise new threats. The study explores the inherent drawbacks of signature-based techniques through a thorough examination, especially with regard to zero-day attacks, which are undetected because no signatures were present when they were discovered. The goal of the study is to evaluate how well IDS rule sets can adjust to the constantly changing threat landscape by examining how well they identify existing vulnerabilities as well as zero-day exploits. The report also emphasises the need of assessing IDS capabilities in light of newly developing security issues, stressing the necessity of creative solutions to deal with the ever-changing nature of cyberthreats. The study adds to the larger conversation on cybersecurity by illuminating the limitations and continued usefulness of signature-based intrusion detection systems. This information helps shape strategic approaches aimed at bolstering organisational resilience in the face of constantly changing cyber threats.

CONCLUSION

In conclusion, the integration of Intrusion Detection and Prevention Systems (IDPS) within Software-Defined Networking (SDN) architectures presents a robust approach to network security. While traditional IDPS tools such as Snort offer signature-based detection, the proposed adaptive IPS enhances security by dynamically adjusting block durations based on attack frequency. SDN's separation of control and data planes allows for greater flexibility and adaptability in network management, albeit with security challenges such as DDoS attacks. Despite these challenges, advancements in SDN frameworks and IDPS technologies offer promising solutions to safeguard network integrity and mitigate evolving cyber threats.

REFERENCES

[1] Pratama, Rifqi Fauzan, Novian Anggis Suwastika, and Muhammad Arief Nugroho. "Design and implementation adaptive Intrusion Prevention System (IPS) for attack prevention in software-defined network (SDN) architecture." 2018 6th International Conference on Information and Communication Technology (ICoICT). IEEE, 2018.

[2] Ali, Amir, and Muhammad Murtaza Yousaf. "Novel three-tier intrusion detection and prevention system in software defined network." IEEE Access 8 (2020): 109662-109676.

[3] Girdler, Thomas, and Vassilios G. Vassilakis. "Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks and Blacklisted MAC Addresses." Computers & Electrical Engineering 90 (2021): 106990.

[4] Xing, Tianyi, et al. "Snortflow: A openflow-based intrusion prevention system in cloud environment." 2013 second GENI research and educational experiment workshop. IEEE, 2013.

[5] Shaghaghi, Arash, Mohamed Ali Kaafar, and Sanjay Jha. "Wedgetail: An intrusion prevention system for the data plane of software defined networks." Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. 2017.

[6] Tasneem, Aaliya, Abhishek Kumar, and Shabnam Sharma. "Intrusion detection prevention system using SNORT." International Journal of Computer Applications 181.32 (2018): 21-24.

[7] Nitin, Tiwari, Solanki Rajdeep Singh, and Pandya Gajaraj Singh. "Intrusion detection and prevention system (idps) technology-network behavior analysis system (nbas)." ISCA J. Engineering Sci 1.1 (2012): 51-56.

[8] El-Hajj, Wassim, et al. "On detecting port scanning using fuzzy based intrusion detection system." 2008 International Wireless Communications and Mobile Computing Conference. IEEE, 2008.

[9] AlMasri, Tamara, Mohammad Abu Snober, and Qasem Abu Al-Haija. "IDPS-SDN-ML: An Intrusion Detection and Prevention System Using Software-Defined Networks and Machine Learning." 2022 1st International Conference on Smart Technology, Applied Informatics, and Engineering (APICS). IEEE, 2022.

[10] Bhardwaj, Anurag, et al. "Network intrusion detection in software defined networking with self-organized constraint-based intelligent learning framework." Measurement: Sensors 24 (2022): 100580.

[11] Chi, Ruinan. "Intrusion detection system based on snort." Proceedings of the 9th International Symposium on Linear Drives for Industry Applications, Volume 3. Springer Berlin Heidelberg, 2014.

[12] H. Holm, "Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter?," 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 2014, pp. 4895-4904, doi: 10.1109/HICSS.2014.600.