Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 7, Issue 2, August 2024
www.ijict.edu.iq
ISSN:2222-758X
e-ISSN: 2789-7362

SNORT VERSUS SURICATA IN INTRUSION DETECTION

Dhuha Sabri Ghazi [1], Hamood Shehab Hamid [2], Mohammed Joudah Zaiter [3], Ahmed Sabri Ghazi Behadili [4]

[1,3] Department of Computer Engineering Techniques, Middle Technical University, Baghdad, Iraq.
[2] Department of Space Technology Engineering, Middle Technical University, Baghdad, Iraq.
[4] Department of Renewable Energy, Al-Karkh University of Science, Baghdad, Iraq.
bbc0067@mtu.edu.iq[1], drhamood@mtu.edu.iq[2]
mjzaiter@mtu.edu.iq[3], eng.ahmed.sabri@kus.edu.iq[4]
Corresponding Author: **Mohammed Joudah Zaiter**
Received:14/06/2024; Revised:07/08/2024; Accepted:20/08/2024
DOI:10.31987/ijict.7.2.290

***Abstract*- In the contemporary digital age, the increasing complexity and frequency of cyber threats underscore the need for efficient network intrusion detection systems (NIDS). This paper provides a comprehensive comparative analysis of two prominent NIDS, Snort and Suricata, focusing on their architecture, detection capabilities, and performance metrics. It explores the historical development, operational frameworks, and technological foundations of these systems, highlighting their respective benefits and limitations in different network environments. Snort, known for its extensive rule-based detection, and Suricata, which leverages multi-threading for high-speed traffic handling, are evaluated based on specific security requirements, including traffic volumes, processing speeds, and threat types. The paper also discusses future advancements in NIDS, particularly through the integration of machine learning and AI, to enhance predictive and adaptive capabilities. This analysis aims to inform cybersecurity professionals about the qualifications and capabilities of Snort and Suricata, providing insights for their effective deployment in modern network security infrastructures. The discussion on future trends emphasizes the importance of continuous improvement in NIDS to address evolving cyber threats).**

keywords: **Snort, Suricata, Intrusion, Detection, Cyber-Security.**

I. INTRODUCTION

In the modern era, one of our ways of life is to operate within a heavy digital environment, intertwining all systems with each other around us not just as an intersociety but also from the business, education, and entertainment sectors. Hence, it stresses greatly upon having secure networking devices. The scale of modern networks brings unique security and reliability challenges [1] that only increase as network complexity grows. If that is not alarming enough, Cybersecurity Ventures estimates the damage caused by cybercrime will soon exceed over 6$ trillion globally per year, calling for stronger defense mechanisms in network protections. It is not uncommon to find firewalls, antivirus software, and even secure socket layer authentication in most organizations, but distinguishing between benign network traffic and malicious ones can be tricky. In the face of increasingly sophisticated cyber threats, traditional security measures do not provide a sufficient level of protection, making Network Intrusion Detection Systems (NIDS) essential [2]. Instead of simply checking packets for values in specific locations within the packet, NIDS monitor network traffic and attempt to find irregular behavior that goes unnoticed by traditional IDS mechanisms [3]. They inspect both inbound and outbound communications, looking for patterns or deviations from normal communication, making them an effective solution against threats like trojans, backdoors, malware, and cyber-spying. Additionally, NIDS are necessary for detecting more sophisticated cyber-attacks, including APTs and polymorphic malware, which cannot be handled by current security systems [4]. APTs, for example,

ISSN:2222-758X
e-ISSN: 2789-7362

are stealth attackers that breach networks and lie dormant long enough to evade traditional security tools. These behaviors are tackled by NIDS, which offer proactive and dynamic security techniques [5].

Essentially, NIDS are a crucial part of cybersecurity practices, supplementing traditional methods by providing an architecture for recognizing potential risks before they lead to security incidents. As threats continue to grow more sophisticated, so must NIDS with advanced techniques like heuristic detection methods and traditional signature analysis to enhance organizational security. These systems should eventually have the ability to protect your network from internal and external threats. Given that cyber threats are advancing at a sophisticated level, both tactics and technologies for responding must also evolve to be an element within a comprehensive digital ecosystem security approach [2]. Table I shows the descriptions of the abbreviations mentioned in this article. The rest of this paper is structured as follows: Section II discusses the importance of network security, especially considering the digital-based nature of many aspects of life. Section III addresses the challenges faced by network security, highlighting the complexity and dynamism of the modern threat landscape. Section IV introduces related work, providing context and evidence. Sections V provide the evaluation metrics of security performance. Section VII offers a comparative analysis of the two, detailing their efficiency in various setups and environments. Section VI discusses the challenges and limitations of IDS and Snort. Section VII elaborates on future considerations, including AI and machine learning integration. Section VIII concludes the paper, emphasizing the implications of the findings.

TABLE I
ABBREVIATIONS & DESCRIPTIONS.

Abbreviation	**Description**
NIDS	Network Intrusion Detection System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
APT	Advanced Persistent Threat
HTTP	Hyper Text Transfer Protocol
FIXIDS	IPFIX-based Signature-based Intrusion Detection System
RAM	Random Access Memory
DOS	Denial of Service
DDOS	Distributed Denial of Service
IOT	Internet of Things
QoS	Quality of Service
IPFIX	Internet Protocol Flow Information Export
UDP	User Datagram Protocol
CPU	Central Processing Unit
WSN	Wireless Sensor Network

II. BACKGROUND

A. *Importance of Network security*

Today, the world has grown so interconnected that the pillars of business, governance, education, and personal interaction have become inextricably linked to digital systems and data exchange. An ever-growing number of organizations and individuals leverage internet-based technologies for their day-to-day routines. When the scope of interaction between

ISSN:2222-758X
e-ISSN: 2789-7362

human life and digital systems expands, the number of vulnerabilities grows as well, multiplying the risk of cyber-attacks exponentially [6]. Thus, network security has transitioned from technological necessity to a vital element of organizational integrity and business continuity. The initial defenses against a host of threats, including breaches, unauthorized access, and attacks, have a significant financial impact, digitize and loss of sensitive information, and public image [7]. A cyber-attack, if successful, may lead to the theft of financial information and intellectual property and disrupt essential systems and services, rendering the business inoperable [8]. Damage may extend far above simple financial losses and influence long-term business operations and prospects [9]. Moreover, the threat does not stay still and continues to evolve, with cybercriminals constantly develop new techniques, including ransomware [10], phishing [11], and APT to exploit any network vulnerability [12]. Therefore, adaptive network security that is not only reactive but proactive is crucial [13]. It is meant to identify potential vulnerabilities, recognize intrusion patterns early, and mitigate exposure efficiently until they turn into full-blown security incidents. Nowadays, network security also intersects with the realm of compliance and legal oversight. Regulative bodies around the world establish increased liability, issuing hefty penalties for non-compliance. It is critical for an organizationâs network security to avoid substantial fines and maintain a legal standard that protects consumer information and privacy [14, 15]; this sustains an organizationâs credibility and relationships with stakeholders and regulatory bodies are maintained. In essence, network security is no longer a means to safe- guard tech properties but an essential tool for strategic risk management and compliance within an enterprise. It is not only the means of protecting vital data and securing tens of thousands of dollars but is essential to guarantee the proper functions and protection of digital systems that people rely upon more and more. Thus, investing in and updating network security is no longer a precaution, it is a vital rule for any organization in the growingly digital-dependent world.

B. Challenges in Network Security

The realm of network security has consistently faced a plethora of challenges, among which include the detection and neutralization of advanced persistent threats (APTs), zero-day exploits, and distributed denial of service attacks, to mention just but a few [16]. APTs can be especially lethal given that they are prolonged and targeted cyber campaigns against specific victims with the intention to steal invaluable information or incapacitate the victimâs operations over an extended period [17]. Their stealthy nature, in which they slowly develop within the victimâs domains for an extended time unnoticed, renders them undetectable by the normal security measures. Another significant challenge is the zero-day exploits in which attackers take advantage of vulnerabilities in software that are not yet detected by the software developer prior to the exploitation time [18]. Since such vulnerabilities are not known to the manufacturer at the time of exploitation, there are no patches or fixes available to prevent the attack, meaning that the attacks bypass the traditional layers of security such as antivirus and firewalls [19]. Distributed Denial of Service Attacks, including overwhelming systems, servers, or networks with traffic to incapacitate them and deny service to legitimate users, have also grown significantly in their scale and sophistication [20]. The simplicity in launching such an attack and availability of cheap DDoS-for-hire services have made the attacks much popular among cybercriminals. The volume and the intensity of DDoS attacks have been on the rise, with many organizations struggling to mitigate the effects due to insufficient bandwidth and the lack of advanced

ISSN:2222-758X
e-ISSN: 2789-7362

protective technology. It is evident that traditional security solutions including firewalls and antivirus cannot be sufficient in the presence of dynamic threats. While firewalls are very effective in controlling access based on pre-established rules, they may lack real-time analysis capabilities to identify and stop the use of crude hacking techniques. Antivirus software, mostly effective against signatures of known malware, cannot stop new and unknown threats, more especially the mutated threats. Besides, most of the signatures have to be detected and fed to the antivirus after the formation of an actual threat, which implies a clear window of opportunities for the first attackers. Clearly, network security for the future needs more proactive, efficient, and sophisticated threat detection and response systems [21]. Such systems, must monitor the networks continuously for any anomaly, a potential indicator of the presence of APTs, zero-day exploits, and DDoS attacks. Artificial intelligence and machine learning models should be integrated to inform the systems of new threats and constantly update their signature databases used in predictive analysis of threats. Logs of vulnerabilities detected in this case may be utilized in running parallel systems that critically sense and report the actual breaches detected. The aim should be to pass the alerts faster, making it difficult for the cybercriminals to exploit detected threats before the protective networking systems have identified and stopped the threats.

C. Role of Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDSs) are critical systems in modern network security because they are used to detect and prevent unauthorized access and malicious activities in network environments. Generally, IDS is designed to analyze network traffic and systemsâ activities to identify un- usual behavior, which could be indicative of a security threat [22, 23]. IDS are, therefore, designed to examine the traffic passing through the network and use predefined rules or known malicious patterns to label the data. The theory behind this approach is that traditional IDS depends on signature-based detection, which matches predefined signatures of known threats against the ob- served network activity. The evolving nature of cyber threats and the corresponding technologies have led to sophisticated methods that evade signature-based detection, forcing a shift to better detection methods [2]. The shift has seen the industry move from signature-based detection only to anomaly-based detection methods and machine learning algorithms [24, 25]. Anomaly-based detection studies the normal network traffic behavior and flags out any deviations as a threat. Thus, anomaly-based detection is best suited to identify Zero-Day Exploits and APTs [26]. Moreover, machine learning continues to improve the adoption of IDS systems. ML allows IDS to learn the network patterns over time and predict threats more reliably [27]. Evidently, computer algorithms are better placed to analyze vast volumes of data to detect anomalies that would otherwise be missed by conventional detection systems. As such, this reduces inaccurate predictions quantified as false positives. The following evolutionary path not only supports IDS roles in networking but also demonstrates the need for further involvement in modern threats. IDS play a more advanced role in network security as administrative filter systems offer continuous monitoring and automated feedback to prevent the loss of network resources by unauthorized users, especially with the in- corporation of machine learning and anomaly detection [28]. This is because IDS must always be prepared for the evolving technological space, as shown by the modern threat culture.

ISSN:2222-758X
e-ISSN: 2789-7362

D. Snort

Snort was introduced in 1998 by Martin Roesch and has since become a pioneering NIDS creation [29]. At first, it was little more than an open-source packet sniffer, but Snort became a powerful standalone intrusion detection system after various enhancements. Snort has been modified numerous times since its inception, and its functionality has now grown to the point where it may be employed in a variety of conditions. These amazing characteristics have enabled Snort to become one of the most successful intrusion detection systems now available, and Snort is used by countless people and businesses, including the majority of government agencies and commercial companies. A three-part modular design, including a packet decoder, a detection engine, and an output module, enables Snort to make sense of network traffic quickly. This modular construction enables the user to apply relatively complex policies and cover a wide range of threats, varying from DoS attacks to unusual means of intrusion [30]. Snortâs modifiability, on the other hand, is its defining feature. The rule-dependent language permits users to swiftly construct complex logic for discovering a variety of disruptive and suspicious operations. It can swiftly evolve to accommodate a wide range of dangers and dangers due to frequent modifications in the detection rules. Snort also includes signature-based discovery, which is used to examine the raw packets for defined harmful data sequences, and anomaly-based discovery, which matches packets with a known baseline criterion [31].

The usage of Snort is extensive and versatile. It serves as a simple packet logging tool, a network intrusion detection system, and a network intrusion prevention system that, under the right configuration settings, is capable of blocking discovered threats. Its functionality through practically all types of network environments from small local ones to vast enterprise networks makes it a perfect fit for every level of network security needs. Its practicality and efficiency have been proven via years of testing and implementation, and positive feedback from thousands of users who have successfully managed to apply it to solve multiple network security needs. The architecture presented in Fig.1 shows an Snort architecture diagram. Snort architecture is the architecture of a Network Intrusion Detection System. At the core of its architecture are the components that make the network data flow easier and facilitate the intrusion detection aspect. To understand those components, it is helpful to understand the flow of network data that is analyzed. Initially, the network data will first flow through the Sniffer component, which is responsible for "sniffing" or intercepting all the packets that pass through the network backbone.

Then, the preprocessed data from the pluginâs activity is passed to the "Detection Engine". The function of the "Detection Engine" as its name implies, is to detect possible malicious or suspicious patterns or known attack vectors in the incoming data. This functionality is achieved using a collection of "Rulesets". The rulesets are the Snortâs core detection activity. They are highly configurable and updated constantly. This allows the snort to be versatile and robust at keeping up with new security threat vectors. Finally, the "Alerts/Logging" function is triggered when a possible threat was determined. Based on the setting, the snort can issue alerts to the system administrators. Alternatively, the snort can simply log the disturbances into "Log Files/Database". Sequential architecture of snort allows to efficiently detect and log intrusions. It stands in the root of monitoring and up keeping the network security infrastructure.

ISSN:2222-758X
e-ISSN: 2789-7362

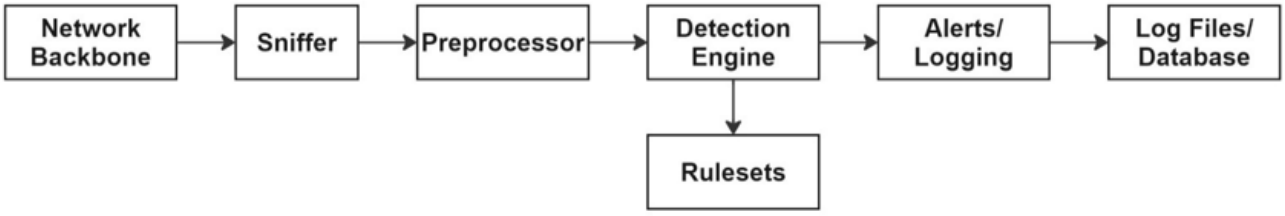

Figure 1: Snort Architecture.

E. Suricata

Several Suricata features align themselves with the current network security requirements. Suricata is described as a next-generation Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) tool that requires performance and security effectiveness [32]. Unlike traditional IDS tools, Suricata has an advanced capacity that allows it to analyze netflows in multiple threads and utilize recent hardware capabilities to ensure maximum traffic flow, thus handling voluminous packets efficiently [32]. The framework's core design is a powerful multi-thread processing pipeline with stages including decoding, flow and stream management, detection, and output. The architecture leverage's multi-core processing power, enhancing its ability to manage high-speed flow and accurately detect threats. The detection capability is supported by a rich set of features such as file identification, extraction, protocol identification, SSL/TLS inspection, and automatic protocol detection. The behaviour used by NIDS/NIPSs will vary depending on the capability and method used.

The rule engine in Suricata has a great affinity to apply the most advanced matching strategies, such as state and anomaly detection paramount in unearthing new threats [33]. Additionally, matching it with scaling and other IDSs facilities and logging software that are compatible, elevate Suricata's effectiveness even further. In conjunction with common use in a corporate network space as an IDS/IPS tool to defend it from breach, network security appliances to identify hazards in real-time, and a tool in query conditions for effective traffic inspection, Suricata also acts with Threat Intelligence Systems to detect more broadly and analyze threats effectively in the dynamical traffic.

Suricata, a constantly active popular platform, remains a relevant and significant player of modern network security offering specific tools to address multiple cyber threats with accuracy and flexibility. The final architecture of Suricata, demonstrated in Fig.2, offers a dependable NIPS and demonstrates that the illustrated NIPs and IDS confluence is also plausible. Additionally, the analysis offers the suitable process that Suricata follows to assure accurate detection and elimination of threats. Precisely, the device captures packets at the "Packet Capture" dimension where raw packets are taken for greater encapsulation. The next stage involves "Packet Decoding" covering various diverse protocols or formats that are decoded by several data decoders. It allows Suricata to handle various types of networks traffics.

Finally, the "Output" stage is where detected threats are reported, logged, or actions are taken based on predefined response strategies. This last phase may involve, for instance, the alerting of the administrators, blocking of traffic, or synchronization with established security protocols. The description of how Suricata functions distinctly by its architecture does not only

ISSN:2222-758X
e-ISSN: 2789-7362

confirm the tool's resilience to attacks in the multi-layered approach but also adapts to different types of networks, marking it as a strong opponent to network threats.

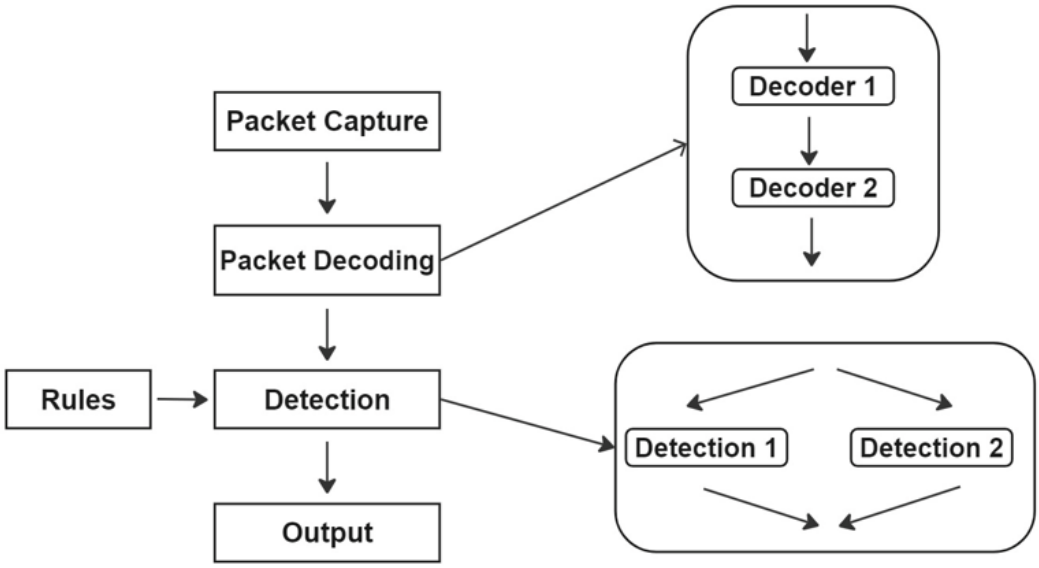

Figure 2: Suricata Architecture

The comparison of the architectural differences between the two IDSs is given in Table II. Specifically, the table focuses on the processing models, and it is possible to see that Snort works on one-threaded architecture. Thus, the system's performance is limited to one CPU core, which affects traffic because all transfer goes through one point. Suricata operates on a multi-threading model that allows using multiple cores for processing and does not make it work on one CPU. Therefore, Snort may not show as good results in cases when the amounts of traffic are too large. The table also provides insight into the systems' scalability and how they handle the data.

According to the table, Snort's linear processing approach may cause packet loss when used in high network conditions. Suricata however, addresses this shortcoming as it will handle the data processing effectively due to its concurrent processing ability. Furthermore, the analysis indicates that Snort may not take full advantage of the modern hardware, while Suricata was developed to work perfectly in the modern multi-core systems, which leads to better performance and efficiency. The insights presented above confirm the reason why the determination of the best system for installation should be based on an end-user and the network environment in which the current platform is based. This determination process plays a significant role in making sure that the chosen intrusion detection system is compatible with the network operations and security services permitted to run.

III. DETECTION CAPABILITIES

IDSs responsible for network security maintenance are crucial, such as Snort and Suricata. These systems take different approaches to identifying unauthorized activities or cyber threats, each possessing unique advantages and disadvantages.

ISSN:2222-758X
e-ISSN: 2789-7362

TABLE II
COMPARATIVE ANALYSIS OF ARCHITECTURAL DIFFERENCES: SNORT VS. SURICATA.

Feature	**Snort**	**Suricata**
Processing Model	Single-threaded	Multi-threaded
Core Architecture	Based on a linear processing pipeline where each packet is processed sequentially	Employs a more complex pipeline that can process multiple packets simultaneously across different threads
CPU Utilization	Limited to using a single CPU core which can be a bottleneck in high traffic scenarios	Can utilize multiple CPU cores effectively enhancing performance in high throughput environments
Data Handling	May struggle with packet drops in high volume networks due to its single threaded nature	Better equipped to handle large volumes of data with reduced packet drops due to its ability to distribute the load
Scalability	Scaling can be challenging; increasing performance typically requires hardware upgrades rather than software configuration	Scales more efficiently by leveraging additional CPU cores, allowing for better performance tuning without necessarily requiring more powerful hardware
Performance in Modern Environments	Might not fully leverage modern hardware capabilities, potentially underutilizing available system resources	Designed to take full advantage of modern multi core systems, potentially offering better performance and efficiency

One of the original IDS software is Snort. This open-source NIDS uses a rule-based language for its signature detection. Snort has well-defined rule sets describing malicious or suspicious activities. When network traffic is erratic with respect to these guidelines, an alert occurs. As a result, Snort is very accurate and can identify any traffic using one of those signatures in its extensive database. However, detecting unknown threats, particularly zero-day exploits, is difficult because there is no rule available to fingerprint them. This is a significant disadvantage since cybersecurity is always evolving. Nazhin et al. pointed out that "no rule exists for zero-day attack, because it is in the early stage and could not be prevented" [34].
Similarly, Suricata is a newer intrusion detection system that has the ability to do more than just Snort's signature-based detection. For example, the process of application layer inspection checks network traffic content, which "is capable of discovering threats within the payload of network packets." This is a deeper level of detection beyond what Snort does with its signature-based method. It is necessary to handle complex threats that can be hidden inside the payload [33]. In addition to its great traffic policing capabilities, Suricata includes protocol anomaly detection. This feature is perfect for situations where command and control communications or data exfiltration attempts are deployed. These cannot be fingerprinted to any pre-existing signatures but are observable through non-standard protocol actions [34]. Also noteworthy is the tool's support for file extraction, allowing monitoring and analyzing files shared through the network for policy or malicious content, identifying malignant files not marked with a signature [34].
The results [34] suggest that both Snort and Suricata versions tested, using given default configurations, do not scale well. An example is Snort in a multi-instance configuration demonstrating scalability. Our testing with Suricata showed a significant improvement in scalability, achieving 52,550 PPS at most for version 1.2, with the new version setting an exceptional record of 258,912 PPS. This makes Suricata between 64,460 PPS at six cores and as much as slightly faster by 9,299 Packets Per Second (PPS) across all configurations than Snort. Our results demonstrate that, significantly in a single

ISSN:2222-758X
e-ISSN: 2789-7362

core setting where we had anticipated Snort to be superior, Suricata outperforms its counterpart. Suricata also obtains lower average memory usage and smaller CPU utilization. Additionally, we considered this at several levels of complexity by altering rulesets and workload, but arrived at the same fundamental principles.

IV. RELATED WORKS

F. Erlacher and F. Dressler (2020) [35] discusses an enhanced version of an IPFIX-based Signature-based Intrusion Detection System (FIXIDS), specifically designed for high-speed networks. FIXIDS leverages HTTP intrusion detection signatures from Snort and applies them effectively to IPFIX-conforming HTTP Flows. This adaptation allows it to handle network data rates that are four times higher than what Snort can manage without experiencing data drops. By offloading a substantial portion of rules and traffic to FIXIDS, the performance of overall security appliances is significantly improved. This approach helps maintain high detection rates while also boosting the systemâs ability to manage larger volumes of data efficiently. Hence, this innovation reflects a major step in network security technology to solve the problem in high-speed network environments of expanding intrusion detection capabilities.

C. Yinka-Banjo et al (2022) [36] sheds light on the high significance of online security to the organizations that promote their business online and the dangers of unauthorized access to it. The efficiency is especially pronounced when IDS is applied for local network protection through statistical or binomial classification methodologies that permit to simplify the detection of attacks. Dumitru supports the further application of this approach due to its effectiveness in recognizing anomalies and intrusions based on the generated outcomes.

A. Gupta and L. S. Sharma (2019) [32] compares the performance of open-source intrusion detection systems Snort and Suricata under high traffic conditions. Snort exhibits lower system overhead and utilizes only one processor core, while Suricata evenly employs multiple cores, providing a higher packet analysis rate. Suricata drops more packets for large packet sizes and high rates of malicious traffic compared to Snort. Additionally, Suricataâs memory utilization depends on both traffic size and malicious input, whereas Snortâs memory usage remains independent of input traffic.

It highlights the significance of computer network security where Erlansari, F. Coastera, and A. Husamudin (2020) [37] introduce intrusion detection systems (IDSs) as a way of automating regular monitoring to notice any illicit activity within netflow data. Software such as Snort, which analyzes network traffic data packets in order to detect intrusions and produce alerts stored in log files, is referred to. In this research paper, Snort was tested to see how well it detected network attacks, and the use of Telegram as a security alarm system for real-time alerting on network attack detection was proposed. A. Waleed, A.F. Jamali, and M.A. Masood (2022) [38] address the problem that NIDPSs are not as efficient in mitigating emerging threats over high-speed traffic, even after consistent signature updates from organizations, due to the surge in attacker activities and the absence of deploying NIDPS with appropriate hardware capabilities on the organization side. It analyzes the results of Snort (single-threaded and multi-threaded), Suricata, and Zeek, three open-source IDPS, on various parameters essential for evaluation. The study, focusing on Small and Medium Enterprises (SMEs), is an extensive literature review not found in previous works, providing complementary information to practitioners and researchers about how IDPS configurations can be tailored to specific requirements.

Abduvaliyev et al [39] discusses factors like traversal path, time, energy, and packet security in Intrusion Detection Systems

ISSN:2222-758X
e-ISSN: 2789-7362

(IDS). It proposes a method aimed at increasing throughput by reducing energy overhead from flooding control messages and other protocol support packets. The existing methods, mostly dependent on hop count and related methods prove suboptimal in a dynamic-changing environments leading to increased latency and packet drop ratios. The proposed method therefore aims at addressing these to maximize network throughput as well as minimizing packet delivery ratios in WSN.
G. Bada, W. Nabare, and D. Quansah (2020) [40] offers detailed comparison of open-source Intrusion Detection Systems with examples of Snort, Suricata, and Bro. As a result, they are tested on multiple types of attacks like DoS and User-to-Root to check how well they can distinguish an attack. The performed experiment is focused on the false positive, false negatives, and true positives alarms for certain network traffic. Overall, the experiment was done under the laboratory conditions in a virtual environment in which all IDS are installed on server with the same characteristic and can analyze the Ethernet speeds up to 5 Gbps.
F. Rafa et al (2022) [41] emphasizes the significance of IDS in protecting cloud-based services from cyber threats, which are increasingly jeopardizing the global IT infrastructure. It highlights the utility of Snort, an open-source IDS, in monitoring network traffic and identifying malicious activities. The research demonstrates the effectiveness of IDS in blocking specific types of protocol traffic such as UDP traffic from source 0.0.0.0:68 to destination 255.255.255:67 thereby preventing unauthorized DHCP address acquisitions and reinforcing network security in cloud computing environments.
S. Adiwal et al (2023) [42] introduces DNS Intrusion Detection (DID), integrated into SNORT, an open- source IDS, to detect major DNS-related attacks, including DDoS-based DNS amplification and tunneling attacks. It presents novel IDS signatures for detecting various attack tools and integrates them into SNORTâs ruleset. Evaluation demonstrates DIDâs high detection rate and low false- positive rate in identifying empirical DNS attacks, enhancing network security against DNS-based intrusions.
A. L. Zhou (2020) [43] enhances the Snort intrusion detection system by improving data acquisition through a third-party interface and enhancing the pattern matching algorithm for improved detection efficiency. Experimental results demonstrate significant improvements in data packet capture capability with a 97.41% reduction in packet loss rate. The improved system maintains a high detection efficiency of 75 M/s, outperforming other algorithms, and successfully detects all alarms for 20 attack scenarios with a maximum response time of only 0.3 s. Overall, the enhanced Snort system proves effective in intrusion prevention and merits widespread practical use.
S. Praptodiyono et al (2024) [44] addresses Distributed Denial of Service (DDoS) attacks in computer networks, proposing a hybrid strategy combining Suricata IDS with pfSense firewall for effective protection. Suricata identifies attack destinations, enabling pfSense to block attacks by dropping malicious packets, resulting in improved Quality of Service (QoS). Results show a 1.08% increase in through- put and a 57.32% increase in the average total number of packets sent, indicating enhanced network performance. The strategy significantly reduces delay and jitter values by 88.78% and 88.99%, respectively, leading to smoother network experiences. Additionally, CPU utilization decreases by 81.23%, showcasing the effectiveness of the combined approach in mitigating DDoS attacks and improving network efficiency.
P. Veerasingam et al (2023) [45] addresses the increasing threat of cybercriminals targeting SME local networks due to limited cybersecurity resources. It advocates for the implementation of an Intrusion De- tection and Prevention System

(IDPS) using Suricata on a Raspberry Pi 2B platform to enhance network security. The study demonstrates Suricataâs effectiveness on low-budget IoT networks with low data traffic, offering real-time intrusion detection and prevention capabilities. Suricata has demonstrated better performance compared to competing systems like Snort, particularly in terms of accuracy and packet loss rate, especially when operated on multi-core architectures. When deployed on OPNsense, Suricata enhances network security for SMEs by preventing unauthorized access and providing timely alerts about network attacks.

The efficiency and application of various intrusion detection systems across different network conditions are reviewed in Table III. This table provides a comparative summary of significant studies, highlighting the models used and their respective outcomes. These findings collectively contribute to the ongoing advancement and optimization of network security measures.

TABLE III
COMPARATIVE SUMMARY OF RELATED WORKS

Ref. No.	Main Idea	Model	Results
[35]	Enhances an IPFIX-based IDS for high speed networks using Snortâs HTTP intrusion detection	FIXIDS	Handles four times higher data rates than Snort without drops, enhancing overall performance
[36]	Highlights the importance of IDS for organizations online, using statistical and binomial classification	IDS with statistical methods	Successfully detects anomalies and intrusions enhancing network security
[32]	Compares performance of Snort and Suricata Suricata under high traffic	Can Snort and Suricata	Suricata uses multiple cores but drops more packets; Snort has lower overhead
[37]	Discusses network monitoring automation automation and intrusion detection using Snort	Snort	Effective in detecting network attacks, integrates with Telegram for real-time alerts
[38]	Evaluates three open-source IDPS for SMEs under high-speed conditions	Snort,Zeek Suricata	Provides insights for optimizing IDPS configurations to meet specific needs
[39]	Proposes a method to increase throughput and security in IDS for WSNs	Custom method IDS	Enhances network throughput and packet delivery ratios
[40]	Comparative analysis of Snort,Suricata, and Bro in detecting various attacks	Snort, Bro Suricata	Detailed evaluation of effectiveness under different traffic scenarios
[41]	Highlights the role of IDS in cloud security using Snort to block specific protocol traffic	Snort	Demonstrates effectiveness in maintaining network security in cloud environments
[42]	Introduces DNS Intrusion Detection in SNORT to combat DNS-related attacks	SNORT with DNS ID	High detection rate and low false positive rate for DNS attacks
[43]	Enhances Snort by improving data acquisition and pattern matching	Enhanced Snort	Reduces packet loss by 97.41%, maintains high detection efficiency
[44]	Combines Suricata IDS with pfSense firewall to mitigate DDoS attacks	Suricata	Increases throughput, reduces delay and jitter, and lowers CPU utilization
[45]	Advocates for using Suricata on Raspberry Pi 2B for SME local network security	Suricata on Raspberry Pi	Shows superior performance in intrusion detection and prevention on IoT networks

V. EVALUATIONS METRICS

Evaluation metrics of security performance are important to understand how effective and efficient a system is, such as Network Intrusion Detection Systems (NIDS). These metrics identify how well a security system protects against and

ISSN:2222-758X
e-ISSN: 2789-7362

responds to threats while reducing false positives. Commonly used security systems performance metrics include:

1) Accuracy: Accuracy measures the overall effectiveness of the system in correctly identifying both attacks and non-attacks. This metric combines the systemâs ability to detect threats and ignore non-threats, providing a comprehensive measure of performance.

$$\text{Accuracy} = \frac{\text{True Positives+True Negatives}}{\text{Total Samples}} \tag{1}$$

2) Precision: Precision measures the fraction of true positive detections among all the identifications made. This metric assesses how many of the flagged incidents are genuine threats, ensuring that the majority of alerts raised by the system are valid hazards.

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives+False Positive}} \tag{2}$$

3) Recall (Sensitivity): Another name for detection rate, Recall is the sensitivity. It illustrates the capability of a system to find true attacks. It evaluates how well the system can detect a large number of real threats, offering great value when assessing threat detection coverage.

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives+False Positive}} \tag{3}$$

4) F1 Score: The F1 Score is the average of both precision and recall, meaning this metric has a balance between the two. It provides a more generalized view of how the model balances precision and recall against each other.

Top of Form

Bottom of Form

$$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}} \tag{4}$$

VI. CHALLENGES AND LIMITATIONS

Despite the position of Snort and Suricata as the powerhouses of intrusion detection, their land is fraught with numerous trials and restrictions. One of the most critical problems is the high rate of false positives and false negatives that scatter their detection competence. Similar to any disingenuous ghost, false positives would classify innocent parishioners as evil spirits, flooding the security team with superfluous alerts and contributing to alarm visual disorder. By contrast, false negatives, the most malignant of malevolencies, slink in the blackness, allowing evil spirits to pass the detection and rolling out the red carpet for other spooks [33].

Another challenge is the necessity to cope with the rising scale and intricacy of networks. As networks grow and traffic becomes more congested, the amount of data grows rapidly. Snort, since it is a single-threaded program, cannot handle such large amounts of data flows, and key detections can be lost. multi-threading is employed by Suricata to rectify this defect; nevertheless, even under such instances, this becomes extremely difficult to work with [46].

Furthermore, systems are subject to robust testing when exposed to extreme scenarios, comprising DDoS attacks in which an uncontrolled increase in data makes it impossible for the systems to keep up, degrading detection quality and increasing false positives. Furthermore, advanced adversaries can outsmart their detection by adjusting their patterns of network traffic, taking advantage of inherent vulnerabilities in existing systems [47].

ISSN:2222-758X
e-ISSN: 2789-7362

Another task that seems very difficult is the maintenance of rule sets and signatures. Not only this task is hardly achievable, but also the process of preserving these systems fresh must be constant: the growing obsolete rules would mean that they create a void for new threats, and the more frequent updates would result in the systemâs destabilization with many false positives [33]. Finally, the issue of encrypted traffic raises significant concerns. With the increase in encryptions in traffic, these systems cannot view into the traffic to scrutinize the contents of packets. Although encryption is a noble way of ensuring privacy, it complicates probing activities by blocking monitoring clusters from getting to the bottom of possibly unfavorable packets buried deep inside [33].

VII. FUTURE TRENDS AND DEVELOPMENTS

In the rapidly evolving field of cybersecurity, intrusion detection systems (IDS) such as Snort and Suricata are essential for defending against increasingly sophisticated and diverse cyber threats. These systems are expected to continue adapting to meet these challenges [48].

Snortâs most well-known feature is its powerful rule-based engine and packet logging for traffic analysis. In future versions, machine learning functionality could become more advanced to better identify anomalies. This will necessitate the use of more sophisticated and self-adjusting artificial intelligence algorithms, which will automatically adjust or generate new rules when new threats arise, reducing human dependency for rule updating. Furthermore, Snort will need to optimize its efficiency and increase its speed in order to process more data while still being able to process the information [30].

According to the several Suricata specialists, and due to its well-known multi-threading and high performance in high-traffic scenarios, one of the likely trends may be to introduce more context into processing. This will likely include data extraction from additional, more diverse sources, such as cloud environments, and Internet of Things devices, which will contribute to a more holistic picture of a possible security threat. Another strong option seems to be further progress on traffic encryption, the weak spot of multiple IDS configurations today [49].

The broader future of IDSs, illustrated by the further development of Snort and the creation of Suricata, will need to reinvent themselves to respond to numerous cases of cyber threats evolving in unprecedented ways. As attackers duly exploit the AI for nefarious goals, the IDS should transition from a reactive to a predictive approach, which means not merely detecting attacks after they occurred but also forecasting and obviating future opportunities to exploit a vulnerability [2].

Moreover, integration of IDS with other components of the security [50-52] infrastructure, particularly with such elements as incident response systems and threat intelligence platforms, will be necessary. It will enable a more unified and quick response to cyber threats.

Additionally, a decrease in the number of machine learning models used for different systems will be likely. Instead, federated learning models may exacerbate and be implemented [1].

Thence, future work will involve the use the Particle Swarm Optimization (PSO) method [53] and Genetic Algorithm with Neural Network and PSO methods [54].

VIII. CONCLUSION

To sum up, this paper provides a comprehensive comparative analysis of two prominent Network Intrusion Detection Systems: Snort and Suricata, which allows us to clarify their distinctive benefits, drawbacks, and differentiated applicability case. Examining the characteristics of the two systems: architecture, detection features, and operation efficiency, we have found that Snort and Suricata are powerful tools for network protection. However, their performance may significantly differ depending on the needs of deployment and operating context.

Snort has been adopted in a broad range of settings and is a useful tool in situations that require well-defined specificity while still providing for extensive customization and rule-based detection capabilities. Snortâs proven utility makes it capable of identifying recognized threats rapidly, encouraged by a vast signature store founded on its extensive use. However, lack of multi- threading does have its drawbacks in high-throughput scenarios and can limit the efficacy of the tool, especially when traffic is abundant and strengthens the systemâs resources. In contrast, Suricata excels in high-traffic environments because of its multi-threaded and overall modern processing model. Its capacity to use multiple cores on a CPU to better access a massive amount of data makes it perfect for large and rapidly changing environments. Furthermore, it has as some essential features that draw extending the work of this tool into the detection of protocol anomalies, the ability to inspect accomplished activities on the application level, and, when required, to extract files. Therefore, it has more capabilities to powerfully combat modern and ever-developing threats. Therefore, the development of adaptive and intelligent NIDS, such as Snort and Suricata is essential as cyber threats grow in complexity and size. Both systems have the potential for great progress in the future, including the improvements in prediction and elimination of emergent threats before the network is affected, and areas related to machine learning and AI.

In conclusion, the choice of Snort and Suricata largely depends on the specific network environment, threat surfaces, and operational considerations. To ensure an effective defense against the emerging and ever-changing cyber threats, organizations should allocate resources to the continuous development and integration of these systems into the comprehensive security framework. Overall, while both options have distinct advantages, the final choice should be based on the strategic security goals, available resources, and planning assumptions for the future cyber environment.

Funding

None

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest

REFERENCES

[1] G. Singh, H. Singh, and A. K. Singh, "A Review Paper on Network Security and Cryptogra- phy," May 2023. [Online; accessed 10. May 2024] DOI: 10.2139/ssrn.4482635 .

[2] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, "A systematic literature review for network intrusion detection system (IDS)," Int. J. Inf. Secur., vol. 22, pp. 1125-1162, Oct. 2023 DOI: 10.1007/s10207-023-00682-2.

[3] Z. Yang, X. Liu, T. Li, D. Wu, J. Wang, Y. Zhao, and H. Han, "A systematic literature review of methods and datasets for anomaly based network intrusion detection," Computers Security, vol. 116, p. 102675, 2022 DOI: 10.1016/j.cose.2022.102675.

[4] N. I. Che Mat, N. Jamil, Y. Yusoff, and M. L. Mat Kiah, "A systematic literature review on advanced persistent threat behaviors and its detection strategy," Journal of Cybersecurity, vol. 10, no. 1, p. tyad023, 2024 DOI: 10.1093/cybsec/tyad023.
[5] G. Laurenza, R. Lazzeretti, and L. Mazzotti, "Malware triage for early identification of Ad- vanced Persistent Threat activities," arXiv, Oct. 2018 DOI: 10.48550/arXiv.1810.07321.
[6] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," Arab. J. Sci. Eng., vol. 45, pp. 3171-3189, Apr. 2020 DOI: 10.1007/s13369-019-04319-2.
[7] O. Aslan, S. S. Aktug, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Electronics, vol. 12, p. 1333, Mar. 2023 DOI:10.3390/electronics 12061333.
[8] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber risk and cybersecurity: a systematic review of data availability," Geneva Pap. Risk Insur. Issues Pract., vol. 47, pp. 698-736, July 2022 DOI: 10.1057/s41288-022-00266-6.
[9] A. Kotidis and S. Schreft, "Cyberattacks and financial stability: Evidence from a natural experiment," 2022 DOI: 10.17016/FEDS.2022.025.
[10] A. Minnaar and F. J. Herbig, "Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the covid 19 pandemic," Acta Criminologica: African Journal of Criminology & Victimology, vol. 34, no. 3, pp. 155-185, 2021 DOI: 10.10520/ejc-crim-v34-n3-a10.
[11] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Front. Comput. Sci., vol. 3, p. 563060, Mar. 2021 DOI: 10.3389/fcomp.2021.563060.
[12] N. I. Che Mat, N. Jamil, Y. Yusoff, and M. L. Mat Kiah, "A systematic literature review on advanced persistent threat behaviors and its detection strategy," J. Cyber. Secur., vol. 10, p. tyad023, Jan. 2024 DOI: doi.org/10.1093/cybsec/tyad023.
[13] M. A. Al Hilmi and E. Khujaemah, "Network security monitoring with intrusion detection system," Jurnal Teknik Informatika (JUTIF), vol. 3, no. 2, pp. 249-253, 2022 DOI: 10.20884/1.jutif.2022.3.2.117.
[14] K. D. Martin, J. J. Kim, R. W. Palmatier, L. Steinhoff, D. W. Stewart, B. A. Walker, Y. Wang, and S. K. Weaven, "Data privacy in retail," Journal of Retailing, vol. 96, no. 4, pp. 474-489, 2020 DOI: 10.1016/j.jretai.2020.08.003.
[15] D. McGraw and K. D. Mandl, "Privacy protections to encourage use of health-relevant digital data in a learning health system," NPJ digital medicine, vol. 4, no. 1, p. 2, 2021 DOI: 10.1038/s41746-020-00362-8.
[16] G. Karantzas and C. Patsakis, "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors," J. Cybersecur. Priv., vol. 1, pp. 387-421, July 2021 DOI: 10.3390/jcp1030021.
[17] N. I. Che Mat, N. Jamil, Y. Yusoff, and M. L. Mat Kiah, "A systematic literature review on advanced persistent threat behaviors and its detection strategy," J. Cyber. Secur., vol. 10, p. tyad023, Jan. 2024 DOI:10.1093/cybsec/tyad023.
[18] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "Zero-day attack detection: a systematic literature review," Artif. Intell. Rev., vol. 56, pp. 10733-10811, Oct. 2023 DOI:10.1007/s10462-023-10437-z.
[19] H. Zare, P. Olsen, M. J. Zare, and M. Azadi, "Operating System Security Management and Ease of Implementation (Passwords, Firewalls and Antivirus)," in Information Technology - New Generations, pp. 749-755, Cham, Switzerland: Springer, Apr. 2018 DOI:10.1007/978-3-319-77028-4-98.
[20] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," J. Sens. Actuator Netw., vol. 12, p. 51, July 2023 DOI: 10.3390/jsan12040051.
[21] M. N. Al-Mhiqani, R. Ahmad, Z. Zainal Abidin, W. Yassin, A. Hassan, K. H. Abdulkareem, N. S. Ali, and Z. Yunos, "A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations," Appl. Sci., vol. 10, p. 5208, July 2020 DOI: 10.3390/app10155208.
[22] J. Diaz-Verdejo, J. Munoz-Calle, A. Estepa Alonso, R. Estepa Alonso, and G. Madinabeitia, "On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks," Appl. Sci., vol. 12, p. 852, Jan. 2022 DOI: 10.3390/app12020852.
[23] H.Y. Kwon, T. Kim, and M.-K. Lee, "Advanced Intrusion Detection Combining Signature- Based and Behavior-Based Detection Methods," Electronics, vol. 11, p. 867, Mar. 2022 DOI: 10.3390/electronics11060867.
[24] D. Samariya and A. Thakkar, "A Comprehensive Survey of Anomaly Detection Algorithms,"Ann. Data. Sci., vol. 10, pp. 829-850, June 2023 DOI : 10.3390/pr11113233.
[25] A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges," Arch. Comput. Methods Eng., vol. 28, pp. 3211-3243, June 2021 DOI: 10.1007/s11831-020-09496-0.
[26] K. Xing, A. Li, R. Jiang, and Y. Jia, "Detection and Defense Methods of Cyber Attacks," in MDATA: A New Knowledge Representation Model: Theory, Methods and Applications, pp. 185-198, Cham, Switzerland: Springer, Mar. 2021 DOI: 10.1007/978-3-030-71590-8-11.
[27] Md. A. Talukder, Md. M. Islam, M. A. Uddin, K. F. Hasan, S. Sharmin, S. A. Alyami, and M. A. Moni, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," J. Big Data, vol. 11, pp. 1-44, Dec. 2024 DOI:10.1186/s40537-024-00886-w.
[28] S. Thapa and A. Mailewa, "The role of intrusion detection/prevention systems in modern computer networks: A review," in Conference: Midwest Instruction and Computing Symposium (MICS), vol. 53, pp. 1-14, 2020.
[29] S. Sharma, P. Nand, and P. Sharma, "Intrusion Detection and Prevention Systems Using Snort," in Advances in Data Science and Management, pp. 473-486, Singapore: Springer, Feb. 2022 DOI: 10.1007/978-981-16-5685-9-46.
[30] I. Karim, Q.-T. Vien, T. A. Le, and G. Mapp, "A Comparative Experimental Design and Performance Analysis of Snort-Based Intrusion Detection System in Practical Computer Networks," Computers, vol. 6, p. 6, Feb. 2017 DOI: 10.3390/computers6010006.
[31] E. Erturk and M. Kumar, "New Use Cases for Snort: Cloud and Mobile Environments," arXiv, Feb. 2018 DOI: 10.48550/arXiv.1802.02359.
[32] A. Gupta and L. S. Sharma, "Performance Evaluation of Snort and Suricata Intrusion Detec tion Systems on Ubuntu Server," in Proceedings of ICRIC 2019, pp. 811-821, Cham, Switzer- land: Springer, Nov. 2019 DOI: 10.1007/978-3-030-29407-6-58.
[33] A. A. E. Boukebous, M. I. Fettache, G. Bendiab, and S. Shiaeles, "A comparative analysis of snort 3 and suricata," in 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET), pp. 1-6, IEEE, 2023 DOI: 10.1109/GlobConET56651.2023.10150141.
[34] J. S. White, T. Fitzsimmons, and J. N. Matthews, "Quantitative analysis of intrusion detection systems: Snort and suricata," in Cyber sensing 2013, vol. 8757, pp. 10-21, SPIE, 2013 DOI: 10.1117/12.2015616.

[35] F. Erlacher and F. Dressler, "On High-Speed Flow-Based Intrusion Detection Using Snort- Compatible Signatures," IEEE Trans. Dependable Secure Comput., vol. 19, pp. 495-506, Feb. 2020 DOI: 10.1109/TDSC.2020.2973992.
[36] C. Yinka-Banjo, P. Alli, S. Misra, J. Oluranti, and R. Ahuja, "Intrusion Detection Using Anomaly Detection Algorithm and Snort," in Illumination of Artificial Intelligence in Cyber- security and Forensics, pp. 45-70, Cham, Switzerland: Springer, Feb. 2022 DOI: 10.1007/978-3-030-93453-8-3.
[37] A. Erlansari, F. F. Coastera, and A. Husamudin, "Early intrusion detection system (ids) using snort and telegram approach," SISFORMA, vol. 7, no. 1, pp. 21-27, 2020 DOI: 10.24167.
[38] A. Waleed, A. F. Jamali, and A. Masood, "Which open source IDS? Snort, Suricata or Zeek," Comput. Networks, vol. 213, p. 109116, Aug. 2022 DOI: 10.1016/j.comnet.2022.109116.
[39] Abduvaliyev, A., Pathan, A. S. K., Zhou, J., Roman, R., & Wong, W. C. (2013). On the vital areas of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys Tutorials, 15(3), 1223-1237. DOI: 10.1109/SURV.2012.121912.00006.
[40] G. Bada, W. Nabare, and D. Quansah, "Comparative analysis of the performance of network intrusion detection systems: Snort suricata and bro intrusion detection systems in perspective," International Journal of Computer Applications, vol. 176, no. 40, pp. 39-44, 2020 DOI:10.5120/ijca2020920513.
[41] F. Rafa, Z. Rahman, M. M. Mishu, M. Hasan, R. Rahman, and D. Nandi, "Detecting Intrusion in Cloud using Snort: An Application towards Cyber Security," in ICCA 22: Proceedings of the 2nd International Conference on Computing Advancements, pp. 199-206, New York, NY, USA: Association for Computing Machinery, Mar. 2022 DOI:10.1145/3542954.3542984.
[42] S. Adiwal, B. Rajendran, P. S. D., and S. D. Sudarsan, "DNS Intrusion Detection (DID) â A SNORT-based solution to detect DNS Amplification and DNS Tunneling attacks," Franklin Open, vol. 2, p. 100010, Mar. 2023 DOI: 10.1016/j.fraope.2023.100010.
[43] A. L. Zhou, "REAL-TIME TRAFFIC DETECTION AND ANALYSIS OF NETWORK SECURITY INTRUSION ATTACK: SNORT INTRUSION PREVENTION SYSTEM," TRE, vol. 79, no. 12, 2020 DOI: 10.1615/TelecomRadEng.v79.i12.30.
[44] S. Praptodiyono, T. Firmansyah, M. H. Anwar, C. A. Wicaksana, A. S. Pramudyo, and A. Al- Allawee, "DEVELOPMENT OF HYBRID INTRUSION DETECTION SYSTEM BASED ON SURICATA WITH PFSENSE METHOD FOR HIGH REDUCTION OF DDOS ATTACKS ON IPV6 NETWORKS. Eastern-European Journal of Enterprise Technologies EBSCO- host," Oct. 2023. [Online; accessed 7. May 2024] DOI: https://doi.org/10.15587/1729-4061.2023.285275.
[45] P. Veerasingam, S. A. Razak, A. F. A. Abidin, M. A. Mohamed, and S. D. M. Satar, "IN TRUSION DETECTION AND PREVENTION SYSTEM IN SME'S LOCAL NETWORK BY USING SURICATA," myjcam, vol. 6, pp. 21-30, Mar. 2023 DOI: 10.37231/myjcam.2023.6.1.88.
[46] E. Albin and N. C. Rowe, "A realistic experimental comparison of the suricata and snort intrusion-detection systems," in 2012 26th International Conference on Advanced Information Networking and Applications Workshops, pp. 122-127, IEEE, 2012 DOI: 10.1109/WAINA.2012.29.
[47] W. Park and S. Ahn, "Performance Comparison and Detection Analysis in Snort and Suricata Environment," Wireless Pers. Commun., vol. 94, pp. 241-252, May 2017 DOI: 10.1007/s11277-016-3209-9.
[48] F. A. Saputra, M. Salman, J. A. N. Hasim, I. U. Nadhori, and K. Ramli, "The Next-Generation NIDS Platform: Cloud-Based Snort NIDS Using Containers and Big Data," Big Data Cogn. Comput., vol. 6, p. 19, Feb. 2022 DOI: 10.3390/bdcc6010019.
[49] H. Asad, S. Adhikari, and I. Gashi, "A perspectiveâretrospective analysis of diversity in signature-based open-source network intrusion detection systems," Int. J. Inf. Secur., vol. 23, pp. 1331-1346, Apr. 2024 DOI: 10.1007/s10207-023-00794-9.
[50] Khudair, Riam Khalil, Ibtisam Ali Hussein, and Bader SS Hamdan. "The Impact of Financial Control Technology in the Banking Business Environment: A Field Study in a Sample of Iraqi Banks." Journal of Techniques 5, no. 3 (2023).DOI: https://doi.org/10.51173/jt.v5i3.753.
[51] Hashim, Hassan Bediar, and Abdul Razzaq Ali Mohammad. "Improving Quality Technological Education Using Web Systems Management Media." Journal of Techniques 5, no. 1 (2023).https://doi.org/10.51173/jt.v5i1.791.
[52] Mhawi, Doaa N., Haider W. Oleiwi, and Heba L. Al-Taie. "Generating Encrypted Document Index Structure Using Tree Browser." Journal of Techniques 5, no. 2 (2023).DOI: https://doi.org/10.51173/jt.v5i2.948.
[53] Khaleel, Hind Z. "Enhanced solution of inverse kinematics for redundant robot manipulator using PSO." Eng. Technol. J 37.7 part (2019).
[54] Khaleel, Hind Zuhair, and Amjad J. Humaidi. "Towards accuracy improvement in solution of inverse kinematic problem in redundant robot: A comparative analysis." International Review of Applied Sciences and Engineering 15.2 (2024): 242-251.

