Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

QUALITY OF SERVICE OF SIGNATURE BASED INTRUSION DETECTION SYSTEM

Durdana Pervez[*1], Dr. Zakira Inayat[2]

[*1,2]*University of Engineering and Technology, Peshawar, Pakistan*

[*1]durdana.pervez@uetpeshawar.edu.pk, [2]zakirainayat@uetpeshawar.edu.pk

DOI: https://doi.org/10.5281/zenodo.21768377

Keywords
Internet of Things, Intrusion Detection System, Signature Based IDS

Article History
Received: 12 January 2026
Accepted: 24 February 2026
Published: 11 March 2026

Corresponding Author: *
Durdana Pervez

Abstract
The intrusion detection systems come loaded with a set of pre-defined signatures; for the majority of organizations these are insufficient, and, even worse, organizations have limited or no time to deal with these suspicious activities, so they often go unattended. Signature-based IDS work by comparing network traffic and system activity against a database of known attack signatures to detect and block malicious traffic. The aim of this research is to evaluate and highlight limitations of signature based IDS. This review paper is primarily aimed to assist researchers by classifying attacks/vulnerabilities of SIDS. The method of attacks and relevant countermeasures are provided for each kind of attack in this work. The pros and cons of different techniques are also discussed. Furthermore, challenges and recommendations are presented in this work.

I. INTRODUCTION
The term Internet of Things basically consists of two words "Internet" and "Things." The internet is the interconnection of computer networks via the standard internet protocol suite (TCP/IP), and it serves billions of users worldwide to access information (audio, video, image, text, etc.). The word "things" refers to any object or person, living or nonliving. Today's communication can be characterized as human to human and human to machine, but Internet of Things communication is considered machine-to-machine communication. As almost every available device is getting smart, the next generation of internet will be the Internet of Things.

Intrusion Detection System is software that manages the network to look for unknown activities, and upon detection these malicious unknown activities are reported accordingly. The five components of intrusion detection are the audit data processor, knowledge base, decision engine, alarm generation, and response. The main purpose of an intrusion detection system is to send an alert/alarm to the system as soon as malicious activity is identified; other tasks include evaluating the quantity and categorizing the malicious activity. IDS provides an additional layer of protection, is a centralized management system, and also manages network routers, firewalls, and files in the database.

Signature based IDS work on pattern matching techniques against signatures already stored in the database; if a match is found, an alert/alarm is generated. Signatures work on known attacks for which patterns are already established. It detects malicious activity that is already saved in the database based on some ruleset and already identified as a threat. The processing speed of signature based IDS is high, as they only detect known attacks and accurately identify malicious activity stored in the catalog. Signature-based IDS

are less flexible in adapting to new threats or evolving attack patterns, as they require constant updates of the signature database. However, signature-based IDS can still be flexible in some ways: the signature database can be updated periodically to include new attack patterns and signatures, and some signature-based IDS have the capability of generating new signatures automatically based on new attacks detected by the system, thus increasing the flexibility of the system.

The accuracy of signature-based IDS is critical in identifying and mitigating security threats. While achieving high accuracy may be challenging, it can be accomplished by ensuring that the signature database is updated regularly, the IDS is configured correctly, and regular performance evaluations are conducted to identify and address any issues. The accuracy of signature-based IDS can be affected by several factors, such as the quality of the signature database, the complexity of the network or system being monitored, and the sophistication of the attacks. Accuracy can also be improved by regularly updating the signature database to include new attack patterns and signatures, ensuring correct configuration for the specific network or system being monitored, and conducting regular performance evaluations and testing to identify areas for improvement.

TABLE I. INTRUSION DETECTION SYSTEM TYPES

Type	Description
Anomaly Based IDS	Detects abnormal behavior and alerts the system when it differs from normal behavior.
Signature Based IDS	Works on a pattern matching mechanism; if the pattern is matched, an alert is generated.
Hybrid Based IDS	Uses both anomaly based and signature based IDS. Signature detects known attacks and anomaly detects unknown attacks.

A. Paper Organization

This paper provides a comprehensive review of signature based IDS, security threats, and solutions for researchers. It covers various applications, security threats, mechanisms, authentication frameworks, and future directions. Section I discusses IoT, IDS, signature based IDS, and related work; Section II is the literature review covering IoT, IDS, signature based IDS, and evaluation of SIDS; Section III covers the research methods and design approach; and Section IV presents findings, discussion, conclusion, and summary.

II. LITERATURE REVIEW

The Internet of Things and its integration with intrusion detection systems has received significant interest within the last few decades. Prior researchers have found that pre-defined signatures pre-loaded into intrusion detection systems (IDS) have certain limitations, such as high resource consumption, low detection accuracy, and false positive or negative rates. For most organizations these are insufficient, and, worse, they don't have enough time or resources to deal with these suspicious activities, which frequently go unnoticed. The literature review begins by interpreting IoT, then connecting it with IDS, and finally signature based IDS and their evaluation.

A. Internet of Things

The term Internet of Things (IoT) was first used in 1999, centered on internet based techniques (1990) [1]. Internet of Things can be defined as the global sharing of information via physically and virtually connected devices. In a sustainable smart city, IoT works as a vital feature. From an architectural or functional point of view, IoT in a smart city is divided into three layers: (i) IoT service layer, (ii) IoT middleware layer, and (iii) IoT infrastructure layer. Over the last decade, IoT in smart cities has been used to develop cost-effective monitoring systems.

IoT is an integral part of the digital-era Industry 4.0 [2]. IoT can be summarized as objects linked and accessed through the internet for the purpose of

sharing information. Ericsson predicted that 18 million devices would be IoT devices by 2022. IoT elements and paradigms are service oriented, things oriented, and sensing/semantic/identification oriented, all converging toward service orientation. The primary objective of IoT is to provide service anytime, anywhere, to anyone. The term Internet of Everything (IoE), coined by Cisco in 2013, considers IoT a vital part of IoE; IoE components include people, data, processes, and things.

The IoT architecture consists of four strata: perception, network, processing, and application [3]. Table II shows the tasks performed by each layer.

TABLE II. IOT LAYERS

Layer	Function
Perception	Monitoring conditions and gathering sensory data; works with sensors such as RFID scanners, surveillance cameras, GPS modules, conveyor systems, and industrial robots.
Network	Facilitates data transfer to the processing layer using systems like WiFi, Bluetooth, Zigbee, LTE, along with protocols like IPv4 and IPv6.
Processing	Responsible for data analysis, computation, decision-making, and storage of large datasets along with cloud servers and databases.
Application	Works for the specific needs of end users as per their requirements.

As more and more devices are connected to IoT, security concerns also increase. The security concerns of IoT can be defined across four major domains: data, communication, architecture, and application [4].

IoT mostly consists of machine-to-machine communication and is easy to exercise at scale [5]. Machine-to-machine communication can send or receive information directly without human intervention. Popular IoT applications include cloud computing, fog computing, edge gateways, edge devices, smartphones, and smart cities. Various IoT security challenges include privacy and data protection, authentication, identity management, trust management and policy integration, authorization and access control, and end-to-end security. Solutions to deal with these challenges include blockchain, systematic key encryption, elliptic curve cryptography (ECC), and steganography.

The current state of IoT security highlights various threats and vulnerabilities that exist in IoT systems, including the impact of cyber-attacks on privacy, safety, and security [6]. Various security solutions and approaches proposed to address IoT security challenges include cryptography, access control, and intrusion detection. Limitations include the limited resources of IoT devices and the lack of standardized security protocols, underscoring the importance of addressing cybersecurity challenges in IoT systems to ensure safe and secure operation.

B. Intrusion Detection System

The security and privacy attacks on IDS can be summarized as shown in Table III [7].

TABLE III. IDS SECURITY ISSUES

Security Issue	Detail
Confidentiality	Interception of message by attackers; trust issue.
Availability	Lack of availability of potential IoT system; connectivity device failure.
Integrity	Original message must not be altered by attacker.

Heterogeneity	Diverse hardware performance and absence of common security services.

Intrusion detection can be a software or hardware tool. It works as a second line of defense, detecting malicious traffic risky to sensor nodes [8]. It also detects and examines machine and user activities and signatures. Its main objective is to create an alert to inform the user, before the intrusion can cause damage, about the intrusion observed in the network or nodes. Attacks can be internal (launched by nodes in the same network) or external (launched by a third party). The three modules are monitoring, analysis and detection, and alarms.

TABLE IV. IOT SECURITY ISSUES

Category	Concerns
Data	Privacy and trust issue.
Communication	Information exchange and information sharing.
Architecture	Authentication and authorization.
Application	Authentication, authorization, exchange of resources, and trust establishment.

Intrusion detection systems are algorithms that alert the system about abnormal behavior [9]. In anomaly based IDS, the normal behavior of the system is evaluated against the observed behavior; its advantage is that attacks are detected before they can execute in real time, though it produces a high number of false positives. Signature based IDS match the data against pre-defined attacks in the system and generate an alert when a signature matches; they are not appropriate for attacks with changing behavior, as they rely on pre-defined attacks already stored in the database.

Current IDS-based approaches for detecting Ethereum attacks have been examined, along with the problems, obstacles, and potential paths for Ethereum security [10]. This includes an examination of each attack's weaknesses, outcomes, and monetary losses, and the usefulness of IDS as a defence against Ethereum assaults. Attackers are always at war, and Ethereum security is continually improving; solutions for detection and categorization are crucial for smart contracts, and deep learning and machine learning approaches are advised to enhance IDS.

IDSs are essential to the resilience and sustainability of networks, though not many have been successful in real-world settings [11]. When it comes to false positives and false negatives, behavioural IDSs require improvement; IDSs ought to be quick to react and not put undue strain on network resources. Behavioural IDSs face issues from overfitting and poor dataset quality. IDS design methodologies include deep learning, machine learning, optimisation, and statistics; neural networks, activation functions, and multi-class classification are methods utilised in the construction of IDSs.

C. Signature Based IDS

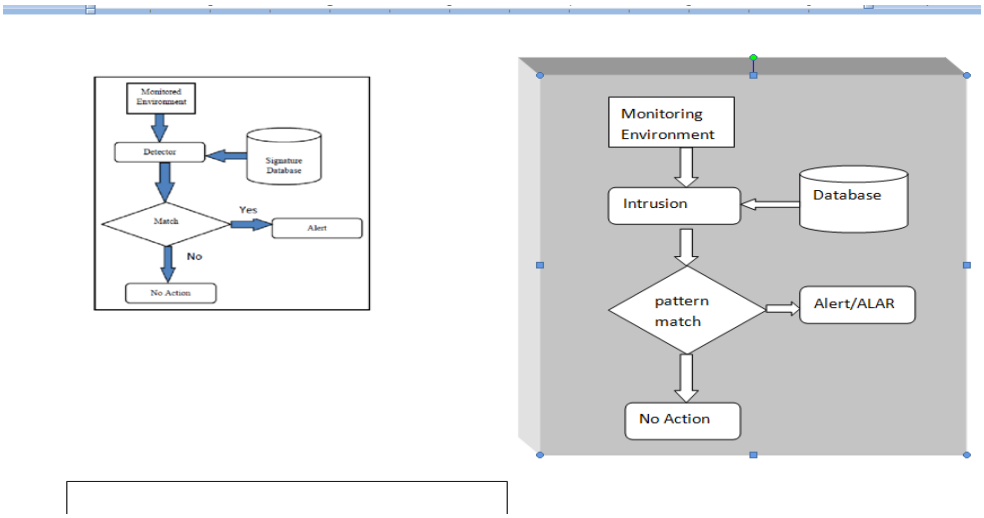


Fig. 1. Signature IDS.

Although signature based IDS are excellent at detecting known attacks, they struggle with zero-day attacks, as these are not stored in the database and matching may not be performed [12]. Zero-day attacks are increasing and malware changes form frequently; in this case, anomaly based IDS approaches give better results.

Signature based IDS, also known as rule based detection, is a simple and straightforward technique that detects patterns already stored in the database against new patterns; if a match is found, an alert is created [13]. Disadvantages include requiring more storage space as attacks grow in quantity, inability to identify new and previously unknown attacks, the need for regular manual pattern updates, its static nature, and the prerequisite of knowledge to form attack patterns.

A study of signature based network IDS for zero-day attacks tested 365 attacks and found that 183 were zero-day based on the rule set and 173 were theoretical [14]. Snort detected 17% of zero-day attacks and 54% of theoretical attacks; attacks already in the signature database share attributes similar to zero-day attacks, which makes detection easier.

Another signature detection technique is attribute based signature, which groups signatures into subgroups based on individual attributes [15]. Within a subgroup, a user can create a signature based on subgroup strategies, and a user with more attributes can belong to different subgroups; results show that user identity remains unidentified during verification.

Signature based IDS, also known as knowledge based or misuse based IDS, work by comparing attacks already stored in the database [16]. Potential benefits include availability of community-supported signature databases, ease of rule comprehension and adaptation, and specific threat information facilitating further investigation. Negative consequences include the need for system expertise for fine-tuning and the significant issue of false positives, which undermines effectiveness; detecting zero-day exploits remains challenging. It has also been reported that 99% of alerts generated by Snort, a popular signature based IDS, are false positives.

A lightweight distributed signature based IDS working on an algorithm for pattern matching of attack signatures has been proposed [17]. The efficient algorithm design helps nodes identify packet payloads and reduces cost, as a lot of pattern matching is avoided; the proposed algorithm is even faster than the WN-Manber algorithm.

D. Evaluation of Signature Based IDS

One of the first developed IDSs was Kalis, with the objective of protecting IoT without consideration of any specific protocol or application used [6]. Kalis is

a network based, online, hybrid (centralized/distributed, signature/anomaly) IDS. Its detection is based on a single network characteristic and it prevents DoS attacks; it also shares information for improved recognition of attacks. Its drawbacks include a single network characteristic requiring more modules for effective detection of multiple attacks, resulting in a sophisticated network, poor performance and accuracy, and the need for more resources. It also has a flexibility problem, as it uses WiFi and requires nodes to be near enough for good performance:

- Poor performance, low accuracy
- Single network characteristic
- More resources needed
- Sophisticated network

Signature based IDS operating with default settings produce a lot of false alarms [18]. To reduce the false positive rate, a scheme has been proposed that adds extra information to network context attack signatures to enhance expressiveness and reduce false positives, using regular expressions to relate context information to interdependent signature patterns. The disadvantage is that it changes the required pattern of signatures, making it more subject to error.

The Suricata Intrusion Detection System was developed in response to the low efficiency of Snort IDS [1]. It was started by the Open Information Security Foundation (OISF) and funded by the US Department of Homeland Security. Its efficiency is improved by working on a multi-threaded framework, and it is flexible as it supports other network standards beyond those specified by OISF. Its drawback is a low detection accuracy rate.

The most commonly used signature based IDS is Snort, which is open source, has a high number of registered users, and is the most dynamic signature based IDS [19]. Snort works with two rulesets known as the Vulnerability Research Team (VRT) and Emerging Threats (ET); by April 2011 these two rulesets had approximately 37,399 signatures. The problem with Snort is its high number of alerts, most of which are false positives, making it time consuming to differentiate genuinely damaging alerts from those unrelated to security incidents of interest.

Two primary deficiencies of signature based IDS have been identified [16]. First, signature based IDS are not capable of detecting zero-day attacks, as the database is not updated frequently, so most malicious activities go unnoticed. Second, signature based IDS generate a lot of false alarms, and the majority of these are false positives; testing shows that 96–98% of alarms generated by Snort are false positives.

Various reasons for the accuracy detection problem of signature based IDS have been identified, the major one being the huge amount of alarms generated, making it likely that the actual alarm indicating a security problem will go unnoticed in the noise of false positives [20]. Detection accuracy also suffers because considerable effort is required to differentiate between normal and malicious network traffic, along with the incapability of IDS to authorize malicious activity as effective or a failure.

Signature based IDS generate a huge amount of alarms, classified as false positive or false negative based on different factors such as IP address, port number, and protocols [21]. Special data mining techniques, including alarm clustering, alarm classification, neural network approaches, and frequent pattern mining, organize voluminous alarms into these categories, making them easier to detect and recover from, and these techniques can be automated. Disadvantages include that these techniques only work offline, labeling of alarms with more than one attribute is not considered, and scalability and the dynamic nature of networks remain drawbacks.

SVELTE IDS is based on both signature and anomaly based detection and works on the IPv6 RPL routing protocol for low-power and lossy networks [22]. It has a centralized module and performs large calculations with resource-constrained modules, and consists of three components: (i) 6LoWPAN for node information, (ii) an analysis and attack detection module, and (iii) a firewall. Its drawbacks are continuous changes of modules in software; it is not suitable for networks with many sensors and does not support distributed module environments.

Vulnerability signatures have been proposed to improve the detection accuracy of signature based IDS [23]. Traditional signature based IDS are unable to detect metamorphic and polymorphic attacks, as

they work on strings and regular expressions for pattern matching, whereas vulnerability signatures work on semantics for pattern matching to detect complex attacks. Compared with conventional regular expression approaches, vulnerability signatures achieve higher detection accuracy and reduce false alarms because of semantic (language) information, though genuine execution as free source software still lacks maturity.

The major concerns of intrusion detection systems are accuracy, false alarm rate, and efficiency [24]. Signature IDS are effective at detecting known attacks, as signatures are already stored in the database, but when pre-defined rules are followed without configuration, detection accuracy increases along with the false alarm rate. To reduce false positives, various scholars have suggested manually disabling some rule sets, though this manual process is costly and time consuming; an alternative is to use a customized rule set based on the operating environment to increase detection and reduce false positives. Different IDS detect diverse attacks as they use dissimilar rule sets.

III. RELATED WORK AND METHODOLOGY

An IDS using Snort (a signature based IDS) with the IDEVAL dataset has been proposed, since traditional firewalls are no longer sufficient for the security needs of increasingly advanced networks [25]. Snort audits network packets as a network signature based IDS and its database must be updated regularly; it recognizes malicious activities by analyzing network communication, and its model and rules can be modified and written in any language. Experimental results show that alerts detected by Snort with the IDEVAL dataset totaled 6612, of which 6334 were false alarms.

A Snort based hybrid IDS combines Snort with two statistically anomaly based algorithms, ALAD and LERAD, targeting distributed denial of service (DDoS) attacks [26]. Experimental results with the EDADT algorithm showed sensitivity of 92.51%, specificity of 88.39%, accuracy of 95.31%, and a false alarm rate of 0.72%; client waiting time was overcome using the HOPERAA algorithm.

A hybrid Snort combining three anomaly based algorithms (ALAD, PLAD, and LERAD) was tested on the KDD Cup 99 dataset [27]. Snort alone detected 77 of 180 attacks; combined with PHAD, detection rose to 105/180; combined with PHAD and ALAD, it rose further to 124/180; and combined with PHAD, ALAD, and LERAD, 149/180 attacks were detected, with a detection rate of 98.88% and a false alarm rate of 0.5529%.

A dynamic multilayered intrusion detection system using a mobile agent showed success on a small database at fixed intervals [28]. Snort was chosen for implementation with an SQL database, and a simple algorithm was designed for both primary and secondary databases; two hardware platforms were used, targeting denial-of-service (DoS) attacks, with tools including IDS-wakeup, Stick, Sneeze, and Nikto. Results showed a 97% decrease in dropped packets.

Machine learning algorithms are used for anomaly based IDS and pattern matching algorithms for signature based IDS, whose performance depends on pattern matching algorithms, rulesets, and packet parsers [29]. A five-phase IDS development approach was proposed: characterizing standard signatures, characterizing network traffic as normal or malicious, defining performance metrics, defining rules, and defining a customized pattern matching algorithm. Snort was chosen as the de facto attack signature reference, and 78 DEFCON traces were used for network traffic analysis with four pattern matching algorithms (Aho-Corasick, Knuth-Morris-Pratt, Wu-Manber, and Rabin-Karp); 43–45% and 16–17% of packets contained attack signatures across the tests.

A pattern based intrusion detection (PIDE) model detects attacks based on a defined set of rules, either developed by experts or generated by default [30]. Rule-based systems referenced include NIDES, IDES, and MIDAS; standard parameters distinguish between authorized and unauthorized users. The proposed model builds the dataset and rules using Jess, examines the model, and provides results, detecting only malicious activity without disturbing authorized users; results show 75% accuracy on test data and 100% accuracy on real-time data.

An intrusion detection system for Android, an enhancement of the common Intrusion Detection Framework, consists of four divisions: log file reading, log file analyzing, controlling output, and storage [31]. The Logcat command inserts data for

log file reading, which is transferred to log analysis; the log analyzer decodes the data and invokes the matching engine to detect pattern matches with the database, after which the analyzed data is forwarded to output control and storage. As technology advances, this model includes an updated rule set interface to detect new attacks.

A performance comparison of Snort and Suricata on FreeBSD, Linux 2.6, and virtual Linux found that both are free source software aiming to analyze packets without packet drop [32]. On the TCP protocol with 512-byte packets, Snort outperformed Suricata as network speed increased from 250 Mbps to 2.0 Gbps, with Snort's performance only degrading on virtual Linux, where the packet drop rate reached 55%. Similar results were found for UDP, with Snort's overall performance better than Suricata's, capable of handling 1470 packets efficiently.

A. Proposed Methodologies

The following are the methodologies considered for developing an IDS:

- Signature-based Detection: constructing patterns or signatures representing recognized attacks; an alert is issued when incoming data matches these signatures.
- Anomaly-based Detection: identifying patterns in a system's or network's typical behavior using statistical models or machine learning to establish a baseline and flag irregularities.
- Hybrid Detection: combining anomaly- and signature-based detection to leverage their respective advantages, lowering false positives and increasing detection accuracy.
- Stateful Protocol Analysis: monitoring the status of network connections and examining protocol behavior to identify unusual activity or protocol breaches.

B. Designing Signature Based IDS

A signature-based IDS is designed to detect malicious activity based on pre-defined signatures of known attacks. The following are the step-by-step procedures for designing a signature-based IDS.

1) Scope and Platform: The scope of this IDS is to improve the performance of signature based IDS, based on the observations described in Table V. The platform chosen is Snort, an open-source IDS platform that uses a signature-based approach to detect and prevent intrusions; it can be customized to fit an organization's needs and has a large community of contributors.

2) Define and Test Signature: Signatures are designed using Snort rules; a signature typically includes a header identifying the type of traffic being matched, followed by a set of conditions describing the traffic's characteristics, targeting Distributed Denial of Service (DDoS) attacks. Test data including a variety of known attacks and normal traffic ensures the signature is accurate and does not generate false positives.

3) Monitor and Analyze Traffic: Network traffic refers to the data transmitted over a network between devices. For this IDS, the traffic monitored is web traffic — traffic generated by browsing the internet, accessing websites, downloading files, and streaming media.

Fig. 2. Types of network traffic.

C. Software Tools for Checking Network Traffic

- Wireshark: a powerful, free network traffic analyzer for Windows, Mac, and Linux that captures packets and provides detailed information including protocol, source, and destination.
- GlassWire: a free network monitoring tool for Windows providing real-time traffic visualization

and alerts, with a user-friendly interface and detailed usage graphs.

D. Algorithms for Improving Snort Efficiency

To improve Snort's performance in a Windows environment, the following algorithms and techniques are considered:

- Multi-threading: distributing the processing load across multiple CPU cores to process network traffic more efficiently.
- Rule Optimization: removing redundant or overlapping rules, organizing them logically, and eliminating unnecessary rules to reduce evaluation overhead.
- Hardware Acceleration: offloading processing from the CPU using NICs with hardware offloading capabilities such as TCP/IP checksum offload or packet filtering.
- Fast Pattern Matching Algorithms: implementing efficient algorithms such as Aho-Corasick or Boyer-Moore to speed up signature matching.
- Buffering and Batching: processing packets in batches rather than individually to reduce processing overhead.
- Intelligent Traffic Filtering: using mechanisms such as network zoning to focus analysis on high-risk areas and improve efficiency.
- Real-time Traffic Analysis: prioritizing processing of high-priority or suspicious traffic to allocate resources more effectively.

E. Maintaining the IDS

Signatures must be regularly updated to include new attack patterns and ensure the IDS remains effective against new threats. Administrators are responsible for continuously ensuring IDS components operate as intended, monitoring for security concerns, conducting routine vulnerability assessments, and addressing any vulnerabilities found.

IV. FINDINGS AND DISCUSSION

This section answers the research question raised in the literature review.

RQ1. What are the limitations of signature based IDS?

To answer this question, Table V was created from a systematic literature review.

TABLE V. CURRENT OBSERVATIONS

#	Ref #	IDS / Protocol Used	Observations
1	[6]	Kalis IDS, online and hybrid IDS	Poor performance, sophisticated network, low accuracy, single network
2	[13]	SIDS – straightforward pattern matching	Static mode, massive database, requires regular updating
3	[12]	Accurately detects known attacks using NIDS	Not suitable for zero-day attacks
4	[18]	Scheme adds extra context information to reduce false alarms	Changes signature patterns, making it subject to error
5	[1]	Suricata IDS; multi-threaded framework	Low detection accuracy
6	[19]	Snort IDS – open source, commonly used, flexible	High number of alerts
7	[16]	SIDS – commonly used IDS	Unable to detect zero-day attacks; generates many false alarms
8	[21]	Categorizing alarms to ease detection	Works offline; dynamic nature is a drawback

9	[9]	Attacks detected before execution	High false positives; unsuitable for changing attack behavior
10	[32]	Snort and Suricata	Snort performance low on virtual Linux but overall better than Suricata
11	[31]	IDS for Android	Updated rule set needed for new attacks
12	[30]	Pattern based IDS	Standard parameters used to detect attacks
13	[28]	Snort and SQL, dynamic multilayered IDS	97% decrease of dropped packets
14	[27]	Snort with anomaly-based algorithms	Anomaly based algorithms (ALAD, PLAD, LERAD)
15	[26]	Hybrid Snort IDS	DDoS attacks considered; EDADT algorithm used
16	[25]	Snort with IDEVAL dataset	Snort with IDEVAL detects 6612 alerts

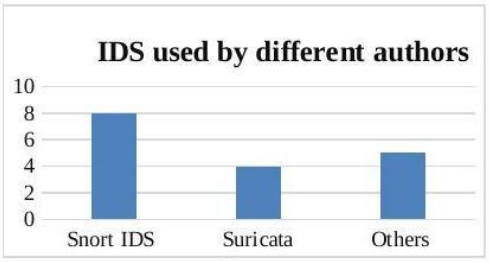
The usage of different IDS across studies shows that, out of 35 studies reviewed, approximately 8 to 10 used Snort, only 4 to 6 preferred Suricata, and the remaining IDS types were used in 5 to 6 studies each, as shown in Fig. 3.

	Steinvall, D. (2022).	IDS	Generate a lot of false alarms
08	Ozkan-Okay, M., Samet, R., Aslan, Ö., & Gupta, D. J. I. A. (2021).	Categorizing alarms makes it easy to detect	Work offline, dynamic nature
			multilayered Intrusion Detection System	packets
14	Khan, K., Mehmood, A., Khan, S., Khan, M.	Snort with different algorithms	Anomaly based algorithms (ALAD,

Fig. 3. IDS used in different studies.

The year-wise distribution shows that, of the 35 papers reviewed, 11 were from 2020, 7 were from 2021, 15 were from 2022, and 2 were from 2023, as shown in Fig. 4.

clearly indicates that out of 35 studies almost 08 to 10 authors used Snort, while only 04 to 06 prefer using Suricata & ratio of



others were 05 to 06 only.

Fig. 4. Year-wise distribution of reviewed papers.

The database-wise distribution shows that the majority of papers were sourced from IEEE and Elsevier, followed by Springer and Google Scholar, as shown in Table VI.

TABLE VI. DATABASE-WISE DISTRIBUTION

Database	Publications
IEEE	8
Wiley Online Library	1
Springer	6
Google Scholar	7
Elsevier	8
Others	5
Total	**35**

V. CONCLUSION

The specific implementation and effectiveness of the algorithms discussed may vary depending on network environment, hardware configuration, and Snort version. Regularly updating Snort to the latest ve rsion and staying informed about performance optimization best practices can also contribute to improving its performance on Windows systems.

Remember that the specific implementation and effectiveness of these algorithms may vary depending on your network environment, hardware configuration, and Snort version. Regularly updating Snort to the latest version and staying informed about performance optimization best practices can also contribute to improving its performance on Windows systems.

6. Summary

This research examine/evaluate signature based Intrusion Detection System to determine their quality based on different factors like (High resource consumption, false positive and negative rates and detection accuracy). As the modern world in becoming globally connected and almost everything is available online therefore the

VI. SUMMARY

This research examines and evaluates signature based intrusion detection systems to determine their quality based on factors such as resource consumption, false positive and negative rates, and detection accuracy. As the modern world becomes globally connected and almost everything is available online, the Internet of Things concept is becoming more common and widely accepted. IoT is the organized collection of intelligent objects that share

information (text, audio, video, etc.); ensuring quality is a primary concern. IoT is present almost everywhere, from homes to offices, health to education, and military to banking, and can be described as a network of smart things for efficient communication. IoT security requirements include confidentiality, integrity, availability, authentication, and backward and forward secrecy.

To deal with the security issues of IoT, intrusion detection systems are widely used. IDS are primarily tools for analyzing network traffic in the Internet of Things; their modules are monitoring, analyzing, and detecting. IDS not only detect attacks but also prevent them through intrusion detection response and prevention systems. The three major types of IDS are signature based, anomaly based, and hybrid based; they can be implemented as hardware or software, and can be host based or network based. An ideal IDS must detect malicious activity, maintain low false positives, and achieve high detection accuracy.

The major drawback of signature based IDS is its failure to detect zero-day attacks, as the database is not regularly updated. Other drawbacks include the storage space required for the large number of signatures, the need for regular updates, and its static mode. Rulesets for pattern matching, such as NIDES, IDES, and MIDAS, can be created by experts or by considering all possible intrusions.

Kalis, the first signature based IDS, has drawbacks related to single and sophisticated network characteristics, poor performance, and low accuracy. SVELTE IDS does not support distributed modules. IP-USN is not suitable for real-time networks. Cloud-Eye, a lightweight IDS, is not suitable for high network traffic and external attacks. A misuse detection model built on the KDD 99 dataset has low detection accuracy. Reducing false positives requires extra information, which increases storage space and requires regular signature updates. Alarm priority techniques that rate and verify false positives face the drawback of unique verification rates, while reference-based techniques for reducing false positives suffer from low detection accuracy. An open-source lightweight Snort configuration has low performance and does not work well for centralized approaches, Bro IDS is not flexible for other operating systems, and Suricata IDS has low detection accuracy.

A new or improved IDS is therefore required to overcome the above-mentioned drawbacks. As future work, we propose implementing various hybrid techniques and machine learning algorithms to improve the performance of signature based intrusion detection systems.

VII. REFERENCES

J. Díaz-Verdejo, J. Muñoz-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," Applied Sciences, vol. 12, no. 2, p. 852, 2022.

P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of things: Security and solutions survey," Sensors, vol. 22, no. 19, p. 7433, 2022.

M. I. Mahmud, A. Abdelgawad, V. P. Yanambaka, and K. Yelamarthi, "Packet drop and RSSI evaluation for LoRa: An indoor application perspective," in Proc. 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), 2021.

A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," Computer Networks, vol. 183, p. 107593, 2020.

K. Wójcicki, M. Biegańska, B. Paliwoda, and J. Górna, "Internet of Things in industry: Research profiling, application, challenges and opportunities—A review," Energies, vol. 15, no. 5, p. 1806, 2022.

A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," Cybersecurity, vol. 4, pp. 1-27, 2021.

Y.-S. Jeong and J. H. Park, "Security, privacy, and efficiency of sustainable computing for future smart cities," J. Information Processing Systems, vol. 16, no. 1, pp. 1-5, 2020.

J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," J. Information Processing Systems, vol. 16, no. 4, pp. 975-990, 2020.

T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. A. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: A review," Procedia Computer Science, vol. 171, pp. 1251-1260, 2020.

A. H. H. Kabla et al., "Applicability of intrusion detection system on Ethereum attacks: A comprehensive review," IEEE Access, vol. 10, pp. 71632-71655, 2022.

M. Alkasassbeh and S. Al-Haj Baddar, "Intrusion detection systems: A state-of-the-art taxonomy and survey," Arabian Journal for Science and Engineering, vol. 48, no. 8, pp. 10021-10064, 2023.

J. Verma, A. Bhandari, and G. Singh, "Review of existing data sets for network intrusion detection system," Advances in Mathematics: Scientific Journal, vol. 9, no. 6, pp. 3849-3854, 2020.

S. Smys, A. Basar, and H. Wang, "Hybrid intrusion detection system for internet of things (IoT)," J. ISMAC, vol. 2, no. 4, pp. 190-199, 2020.

A. Shaikh and P. Gupta, "Advanced signature-based intrusion detection system," in Intelligent Communication Technologies and Virtual Mobile Networks: Proc. ICICV 2022, Springer, 2022, pp. 305-321.

L. Guo and C. Lan, "A new signature based on blockchain," in Proc. 2020 Int. Conf. Intelligent Computing, Automation and Systems (ICICAS), 2020.

T. Sommestad, H. Holm, and D. Steinvall, "Variables influencing the effectiveness of signature-based network intrusion detection systems," Information Security Journal: A Global Perspective, vol. 31, no. 6, pp. 711-728, 2022.

K. Sampoornam, S. Saranya, G. Mohanapriya, P. S. Devi, and S. Dhaarani, "Analysis of LEACH routing protocol in wireless sensor network with wormhole attack," in Proc. 2021 Third Int. Conf. Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021.

Y. Otoum and A. Nayak, "AS-IDS: Anomaly and signature based IDS for the internet of things," J. Network and Systems Management, vol. 29, pp. 1-26, 2021.

J. E. Díaz-Verdejo, A. Estepa, R. Estepa, G. Madinabeitia, and F. J. Muñoz-Calle, "A methodology for conducting efficient sanitization of http training datasets," Future Generation Computer Systems, vol. 109, pp. 67-82, 2020.

D. N. Mhawi, "Modified ensemble learning algorithms for network intrusion detection system," Ph.D. dissertation, University of Technology, 2022.

M. Ozkan-Okay, R. Samet, Ö. Aslan, and D. Gupta, "A comprehensive systematic literature review on intrusion detection systems," IEEE Access, vol. 9, pp. 157727-157760, 2021.

M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882-6897, 2020.

C. Zhang, D. Jia, L. Wang, W. Wang, F. Liu, and A. Yang, "Comparative research on network intrusion detection methods based on machine learning," Computers & Security, p. 102861, 2022.

S. Rajagopal, P. P. Kundapur, and K. Hareesha, "Towards effective network intrusion detection: from concept to creation on Azure cloud," IEEE Access, vol. 9, pp. 19723-19742, 2021.

S. Kumar Birthriya and A. K. Jain, "A comprehensive survey of phishing email detection and protection techniques," Information Security Journal: A Global Perspective, vol. 31, no. 4, pp. 411-440, 2022.

H. Zhang, Y. Li, Z. Lv, A. K. Sangaiah, and T. Huang, "A real-time and ubiquitous network attack detection based on deep belief network and support vector machine," IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 3, pp. 790-799, 2020.

K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," J. Systems Architecture, vol. 105, p. 101701, 2020.

M. S. Habeeb and T. R. Babu, "Network intrusion detection system: A survey on artificial intelligence-based techniques," Expert Systems, vol. 39, no. 9, p. e13066, 2022.

O. H. Abdulganiyu, T. A. Tchakoucht, and Y. K. Saheed, "Towards an efficient model for network intrusion detection system (IDS): systematic literature review," Wireless Networks, pp. 1-30, 2023.

H. Herath and M. Mittal, "Adoption of artificial intelligence in smart cities: A comprehensive review," Int. J. Information Management Data Insights, vol. 2, no. 1, p. 100076, 2022.

H. Wang, W. Zhang, and H. He, "You are what the permissions told me! Android malware detection based on hybrid tactics," J. Information Security and Applications, vol. 66, p. 103159, 2022.

A. Waleed, A. F. Jamali, and A. Masood, "Which open-source IDS? Snort, Suricata or Zeek," Computer Networks, vol. 213, p. 109116, 2022.