nternational Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): 444-462
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

Survey on Intrusion Detection System Types

Suad Mohammed Othman[1], Nabeel T.Alsohybe[2], Fadl Mutaher Ba-Alwi[3], Ammar Thabit Zahary[4]

Faculty of Computer & Information Technology
Sana'a University, Yemen

suad.m.othman@gmail.com[1], alsohybe@gmail.com[2] , dr.fadlbaalwi@gmail.com[3], aalzahary@gmail.com[4]

ABSTRACT

Intrusion detection system (IDS) is one of amongst the most essential consideration of cyber-security that can discover intrusion before and/or after attack occur. An Intrusion detection system is software or hardware designed to detect any malicious activity or attack against the system or network. The main contribution in this paper is to present an overall review of IDS types that are deployed in various environments. So many IDS researches have mostly described the types of IDS. However, their description has addressed a specific area and there is a lack of researches that present an overall review of IDS types. This paper conducts a review of different types of IDSs related to different environments and platforms through a comparative approach. Also, it presents a classification of IDS types based on criteria such as platform and input data. It introduces their significant features, advantages and disadvantages of each type. The finding out of this survey have been coming from our analysis of the current research and trends of the field. In this paper has addressed the lack of IDS types research and many points of research have been figured out as a future work.

KEYWORDS

Intrusion Detection Systems (IDSs), Host based IDS (HIDS), Network based IDS (NIDS), Hybrid based IDS or mixed IDS (MIDS), Protocol-based IDS (PIDS), Network Behavior Analysis (NBA), Distributed and Collaborative IDS (DIDS), Hypervisor based IDS.

1 INTRODUCTION

As more people use the Internet for personal or business reasons, different cyber-attacks and intrusions are growing by the day. IDS is one of amongst the most essential consideration of cyber-security. IDS is utilized to recognize successful violations even after they have happened [1]. The term intrusion detection system was first used by James Anderson [2] in the late 70s and early 80s. He introduced the concept of misuse detection and predefine events and provided the basic for future IDS design and development. An IDS is software or hardware designed to detect any malicious activity or attack against the system or network. An IDS collect data from different sources within a computer or a network such as system command, system log, system accounting, security log and network log. Then, it analyzes them to identify possible security violation, and finally, it issues an alert to the system administrator to deal with the intrusion. The authors Swathi Pai M, Ashoor et al. [3, 4] summarized IDS Functions as: monitoring and analyzing both the user and system activities, analyzing system configurations and vulnerabilities, evaluating the system and file integrity, recognizing patterns

typical of attacks, analyzing of abnormal activity patterns and tracking user policy violations.
There are two main types of IDS: Network-based IDS and Host-based IDS [5]. NIDS is placed along a network to monitor all network traffic [5]. HIDS placed on a host to scan and monitor the all hosts process or devices on the network [5]. In addition, there are other types of IDS. However, there are little researches that display the most types of IDS. The objective of this paper is to compare and display the different types of intrusion detection systems based on platform and data they collect for detecting intrusion analysis. Then the research will display the advantages and disadvantages of these IDS types to identify leading trends, open issues, and future work possibilities.

The rest of this work is organized as follows: Section 2 explains the classification of IDS. Section 3 lists the types of IDS and comparison between them. Section 4 discussion. Finally, Section 5 concludes this paper.

2 CLASSIFICATION OF INTRUSION DETECTION SYSTEMS

In this section, a survey is presented on IDS types by collecting the most recent researches relevant to the field. Our methodology in this survey is to conduct an overall review for all types related to all environments of IDS and applications. This can be considered the contribution of our paper in addition to the classification of IDS types based on some criteria such as platform that are network, host, virtual machine and hybrid.
Researches of IDS have made good progress. Several studies have described the types of IDS.

Aumreesh et al. [6] introduced a general study of IDS. The authors discussed the intrusion detection and the types of IDS. The research emphasized the range of IDS types such as host, network and hybrid IDS. The authors also, described every single type of IDS.

In their survey, Mayur and Bansode [7] introduced the different types of IDS and classified the types of IDS into the following three types: traditional IDS, IDS for wireless network, and IDS for database. The research divided traditional IDS into three types: HIDS, NDIDS, and hybrid IDS.

Hung et al. [8] introduced a comprehensive review of the Intrusion detection system and classified it into four classes: HIDS, NIDS, WIDS, NBA and MIDS. The study compared the four types based on the following criteria: component, Detection scope, and Network architecture of each class. Table 1 shows details of the four classes and a comparison between them.

Zouhair et al. [9] introduced an overview of diverse intrusions in cloud and different detection techniques used by IDS. The research displayed an overview of the cloud computing types based on IDS and divided Cloud-based IDS into the four types showing in Figure 1.

S. SobinSoniya and S. Maria [5] introduced an overview of IDS Classification and Techniques. The study classified IDS into two main types: NIDS and HIDS. The authors also, classified techniques used in detecting attacks for securing the network from new attacks.

Bruno et al. [10] presented a an overview of IDS for IOT and classified the IDSs based on detection method, IDS location, security threat and validation strategy. In addition, the paper discussed the different possibilities for each attribute, and described intrusion detection techniques for IOT. The research, also, classified the IDSs into two main types: NIDS and HIDS.

IDS types can be categorized into many types based on the deployed platform to detect attacks and depending on the input data that collected from different resources such as system call, audit log, user or system activites, application process, and network traffic to analysis and detect attack. Also IDS can be categorized based on attack type that can be detected by each type.

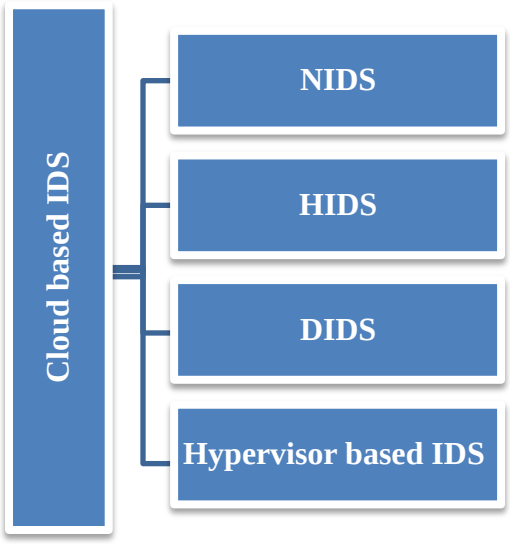

Figure 1: Cloud based IDS [9]

The authors can categoriz IDS types based on the platform and input data into four classifications that are IDS deployed on host or single machine, IDS deployed on the network that is a single machine or multiple machine, IDS deployed on host and network, finally, IDS deployed on virtual machine (VM).

Figure 2 shows the our classification of IDS types based on platform that it deployed in it. Table 2 displays comparative between IDS types based on some criteria's such as platform, input data and the attacks that IDS can detect.

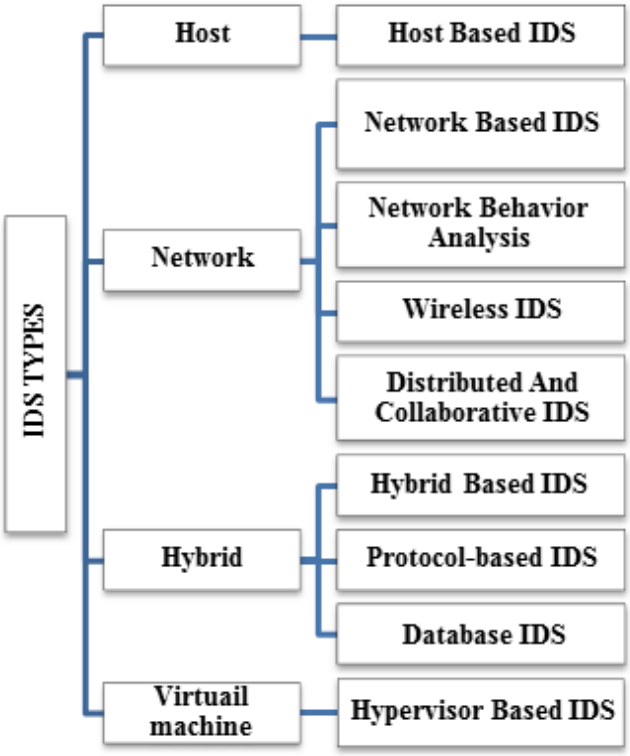

Figure 2: Classification of IDS types.

Table 1 Comparisons of IDS types [8]

IDS	HIDS	NIDS	WIDS	NBA
Components	Agent. Management server. Database server.	Sensor: (inline/passive). Management server. Database server.	Sensor: (passive). Management server. Database server.	Sensor: (most passive). Management server. Database server.
Detection scope	The host	Network or Host.	WLAN. WLAN client.	Network or Host.
Network architecture	Managed networks or standard networks.	Managed networks.	Managed networks or standard networks.	Managed networks or standard networks.

Table 2: IDS types comparative

IDS	Platform	Input data	Attack types that IDS detect
HIDS.	Host	System configuration, application activity, system logs, system command, running processes, file access and modification Security Logs [11].	Key stroke logging, Identity theft, Unauthorized access, Spamming, Malicious process, Botnet activity, Spyware-usage.
NIDS.	Network	Network Traffic packet, Prior events, user profiles	TCP SYN attack, fragmented packet attack [12]. Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) [13]. In [5] the authors classified attack into two types show in Figure 3.
Hybrid based IDS.	Host + Network	According to systems hybrid	According to systems hybrid
Protocol-based IDS (PIDS).	Network (web server) + Host	Normal usage of a protocol, HTTP, Structured Query Language (SQL) protocol [11]. Application-level traffic and commands [14]. Audit records, Data sources of running applications, and Log file.	CANCEL DOS attack, BYE DOS attack, INVITE Request Flooding Attack, Media spamming, RTP packets flooding [15].
Network Behavior Analysis (NBA).	Network	Log traffic over a network. Log system.	DDoS , DoS , unexpected services, Network scanning, policy violations, Source routing attack, malware and flood attack.
Wireless IDS (WIDS).	Wireless network	Wireless network traffic, such as ad hoc network.	Sinkhole attack, Spoofed, altered routing attack, Misdirection, HELLO Flood Attacks, Sybil attack, Wormholes, Selective forwarding , Black-hole attack and Homing attack [7, 16, 17]. BlueSnarf, Bluejacking, BlueBug, Blue Smack [18].

Table 2: IDS types comparative(continued)

IDS	Platform	Input data	Attack types that IDS detect
Distributed And Collaborative IDS (DIDS).	Network	Aggregate information from different sources according to multiple IDS.	Attack that single IDS can't detect such as (DDoS) and its type, doorknob attack, network browsing [19]. large scale stealthy scans, worm outbreaks [20].
Database IDS	Host + Network	user session , user input parameters and SQL commands [21].	SQL injection, direct database attack, Injection attack, privilege escalation attack, and hijack future session attack.
Hypervisor based IDS.	VM	Packet leaving and entering to VM, system log and call, information process running in VM and traffic payload information [22].	VM scape, Guest Dos, CROSS_VM side channel, ,VMM backdoor and hardware attack, VM traffic spoofing, port scanning [22]. Virtualization-specific attacks such as: Insider attacks [23].

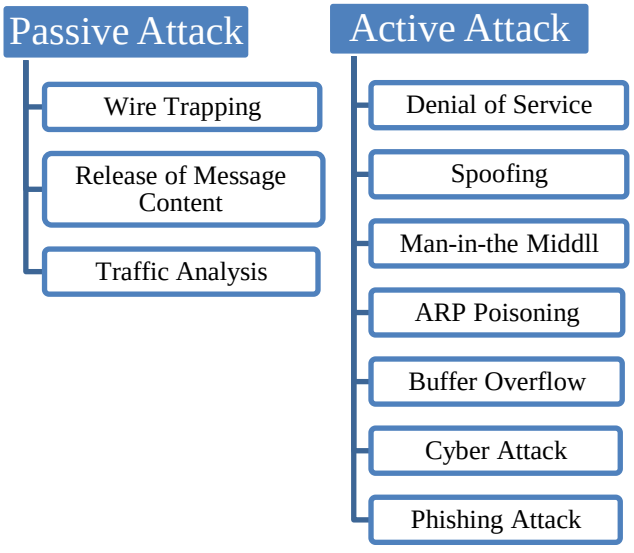

Figure 3: Network IDS attack [5].

3 TYPES OF INTRUSION DETECTION SYSTEMS

There are many types of IDSs, which can be summarized as follows:

3.1 Host based IDS (HIDS)

HIDS was the first developed type of intrusion detection. HIDS monitors and analyzes the internal computing system or system level activities of single host such as: system configuration, application activity, wireless network traffic (only for that host) or network interface, system logs or audit log, running user or application processes, file access and modification. Figure 4 represents the HIDS. The capabilities of HIDS include integrity checking, event correlation, log analysis, policy enforcement, rootkit detection, processor, memory, hard-disk and battery utilization, and alerting [24, 25]. HIDS tends to be more accurate and less false positive than network-based IDS because it analyses the log files, and as a result, it can determine whether an attack successful occurred or not [26]. The Host based intrusion detection system requires programs (or agents) to be installed on the system to generate

reports indicating if any malicious activity occurred. The problem with host-based systems is that they tend to be resource intensive because they use the same computer resources installed on it and don't have operating system independent like other types of IDS [27, 28]. There are many existing systems that introduce host-ID system type, for instance OSSEC [29] and Tripwire [30].

HIDS analyze the audit log files to identify and detect any malicious system processes. However, to analyze a large amount of data to distinguish between normal process and malicious processes, needs a long time of computation and a lot of resources. A lot of researches introduced methods to solve this problem for instances: Marteau [31] introduced a new similarity measurein symbolic sequential data to detect unknown attack. In the proposed method the author focused on sequences of system calls by using Sequence Covering algorithm for Intrusion Detection (SC4ID). SC4ID algorithm based on optimal-covering of a sequence by a series of subsequences extracted from a predefined set of sequences. The SC4ID algorithm was evaluated on UNM and ADFA-LD well-known system call datasets.

Subba et al. [32] introduced framework to improve the efficiency of computation in HIDS. The proposed framework transformed the system call to n-gram vector and then reduced the size of the input feature vectors by dimensionality reduction process. The feature vectors are finally analyzed by various machine learning classifiers that named (Naive Bayes, MLP, C4.5 Decision Tree, and SVM) to identify intrusive processes. To evaluate the proposed model the benchmark ADFA-LD has been used.

Deshpande et al. [33] proposed model to analysed only selective system call traces for detect any malicious activities within the system and then alert the cloud user to found malicious process.

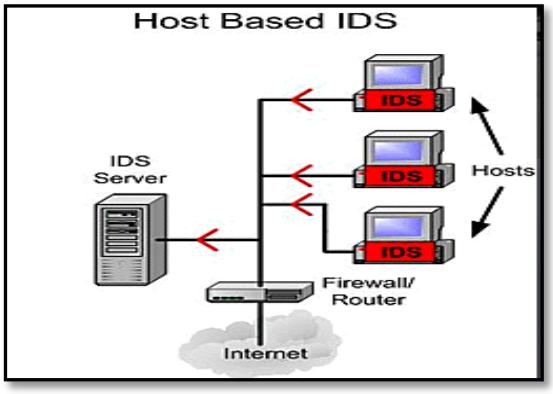

Figure 4: Host based IDS[34].

3.2 Network based IDS (NIDS)

NIDS is used to monitor and analyze network traffic on specific network segment for suspicious activities detection. Figure 5 represents NIDS and its steps in detecting attacks. NIDS used in packet level analysis for all systems in the network segment by check IP, transport-network and application protocol level activities and headers of packet to detect many IP-based DOS attacks like TCP SYN attack, fragment packet attack [12]. NIDS concentrates more on the abuse of vulnerabilities while HIDS center around abuse of privilege [28]. NIDS costs less and quicker in response than HIDS because there is no need to maintain sensor programming at the host level, and it monitors traffic on a real time or on close real time [14]. Therefore, NIDS can detect attacks as they occur. However, NIDS does not indicate if such attacks are successful or not since it doesn't analyze the log system. The problem with NIDS is that it has restricted visibility inside the host machine, and there is no effective way to analyze encrypted network traffic to detect attack [12]. Therefore, until now, many researches progressed to develop effective ways for NIDS to detect attacks. Several products for network intrusion detection exist, such as Snort [35] and NetSTAT [36], which is a tool aimed at real-time NIDS. Until now there are a lot of researches that introduced methods for NIDS such as:

Sklavounos et al. [37] proposed new method of NIDS for DOS attack detection based on the tabular cumulative sum (CUSUM) chart and the exponential weighted moving average (EWMA) chart on the UDP and ICMP source bytes of the experimental dataset NSL-KDD.

Suad Othman et al. [38] proposed intrusion detection model on big data environment using machine learning algorithm named SVM for classification and Chi-selector for feature selection to reduce dimensionality in network traffic. To test the proposed model KDD dataset has been used.

Parvat et al. [39] proposed NIDS using deep learning. In the proposed method has been used an ensemble of multiple binary classifiers which deep learning model with a divide and conquer strategy. To evaluate the system NSL-KDD dataset has been used.

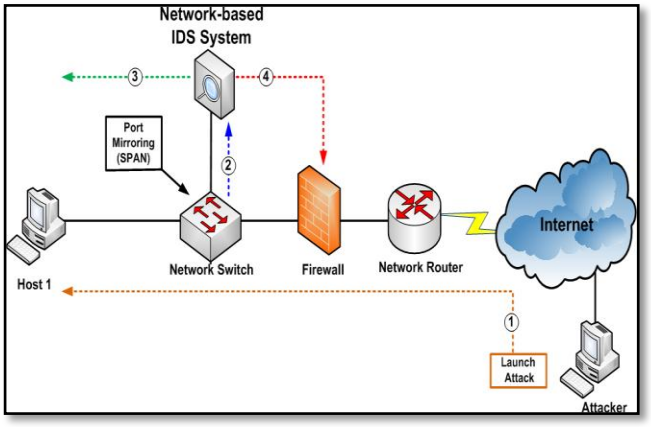

Figure 5: Network-based IDS

3.3 Hybrid based IDS or mixed IDS (MIDS)

MIDS Combines two types or more of IDS to achieve the advantages of IDS and complete an accurate detection [8] such as Double Guard [40] that uses host ids and network IDS. However, MIDS takes a long time in analyzing data. Figure 6 represents Hybrid based IDS.

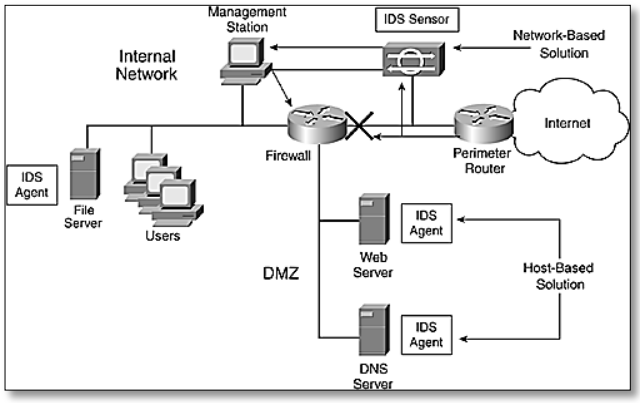

Figure 6: Hybrid based IDS

3.4 Protocol-based Intrusion Detection System (PIDS)

PIDS monitors and checks the specific protocol behavior and its state like Hyper Text Transfer Protocol (HTTP) [11]. PIDS can be specialized to monitor application protocol, which is called APIDS [11]. It focuses on actions that happen in some particular application through monitoring and analyzing the application log files or measuring their performance [41]. There are researches that introduced to PIDS such as: Danish et al. [42] proposed an IDS for the detection jamming attacks in a LoRaWAN network. The system has been implemented based on LoRaWAN protocol.

3.5 Network Behavior Analysis (NBA)

NBA monitors and checks network traffic to know threats that produce uncommon traffic flows, such as DDOS attacks, malware, and policy violations [43, 44]. The NBA system investigates of network traffic to identify attacks with unexpected traffic flows [8]. Sindhu [45] Described NBA as a method which passively monitor the movement traffic in a network for a specific time and forms a standard for normal traffic. Furthermore, the behavior is compared to a standard to find any uncommon activity in a network. NBA systems are most often deployed on internal networks of an organization and are,

also sometimes, deployed where they can monitor flows between an organization's network and external networks [46].

There are many NBA systems such as:

Kakuru [45] proposed a tool for internal network that offers a method to detect any uncommon behavior by an authentic user. In the proposed tool used Wireshark to record log traffic over a network. First, Wireshark recorded the user's activity for a period of time, and stored the record in a database. second, the new activity is compared to the past activity and alerts any new behavior to the administrator. Koch et al. [47] proposed a new NBA by used similarity measurements and insider activities such as data exfiltration in encrypted environments. in the proposed architecture used intrasession and intersession correlation, to determine the similarity between connections.

The advantage of NBA is that it focuses on the overall behavior of the devices on the network; therefore it is allowed to respond to unknown or specific threats for which no signature is available and zero-day attack.

3.6 Wireless IDS (WIDS)

WIDS monitors and analyses wireless traffic to detect any attacks. Wireless traffic is an ad-hoc network, wireless mesh network, and wireless sensor network [8]. There are numerous types of attack in wireless network such as Sinkhole attack, Spoofed altered routing attack, Flood attack and Sybil attack [7]. Figure 7 displays wireless intrusion detection system.

Wireless networks have many features such as existence in the open environment, limited in computational power of sensors, battery life and memory capacity; therefore, IDS produced for wired networks cannot be applied completely to wireless networks [16]. Wireless network is more vulnerable to attacks than wired networks since their infrastructures are dynamic by nature.

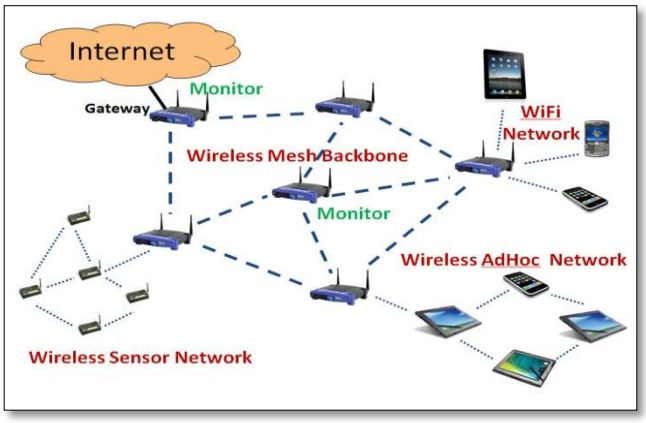

Figure 7: Wireless IDS

Ahmed Patel et al. [41] summarized the advantage and disadvantage of the wired and wireless network, as showing in table 3. The author summarized the aim of applied the IDS for WSN is to detect whether the node from the network is malicious or physical damage. WIDS important to provide integrity, confidentially and availability; therefore, it evaluates the signal jamming and eavesdropping.

Devi et al. [48] used the Adaptive Neuro-Fuzzy Inference System to deal with the security analysis of 5G wireless communication network implementation of IDS and used KDD cup 99 data set for system test.

Kolias et al. [49] proposed a distributed network IDS for wireless networks. The system is based on classification rule induction and swarm intelligence principles to analyzed data for intrusion detection. Aegean wireless intrusion dataset version 2 has been used to test the proposed method.

Gupta et al. [50] used game theory on the small cell access point in 5G wireless to detect bandwidth spoofing attack and analyzed the effect of it. The authors also proposed an adaptive IDS used a hidden Markov Model to detect an intrusion and focused on security issues of the 5G wireless networks.

Table 3: Wire and wireless network advantage and disadvantage [41]

Network	Advantage	Disadvantage
Wired network	▪ It is faster and low cost.	▪ It is deeply dependent on infrastructure platform and not easy to deploy.
Wireless network	▪ It deals wide coverage and unlimited access which implicates openness to attacks. ▪ Wireless networks are scalable and independent from arrangement platform.	▪ The wireless medium itself has to be protected.

3.7 Distributed and Collaborative IDS (DIDS)

DIDS consists of multiple IDS over a network, all of which communicate with each other, or with a central server that enables network monitoring [12].

Figure 8 explains the DIDS. DIDS is designed to work in a not homogenous environment, which means that DIDS provides capability to aggregate information from different sources to detect attacks against a network system such as doorknob attack and DDoS attack. There are three components in the framework of DIDS, which are IDS agent, communication component and central analysis server. DIDS has several advantages compared to the centralized IDS showing in table 4 [41, 51, 52]. There are many researches that covered DIDS such as: Zeeshan and Peter [53] designed and evaluated some distributed IDS methods for IoT that are appropriate to small devices. The authors used a trust management method that allowed devices to manage reputation data about their neighbors. The proposed method made it possible to single out maliciously behaving units in a processing and energy-friendly way.

Steven R. Snapp1 et al. [19] which proposed a prototype DIDS that generalizes the target environment in order to monitor numerous hosts interconnected via a network also the network itself.

Collaborative IDS: distributed IDS have the ability to connect alarms coming from diverse sensors [20]. These intrusion alerts are joint by the correlation unit, then reports are produced, and finally, the actual nature of the attacks is confirmed [20]. This is a potential to make the IDS autonomous, self-adjusting capabilities, parallel, organized and efficient. Isolated IDSs will not be able to achieve connections between malicious actions happening at different places at the same time [54].

Arshad, J., et al. [55] proposed collaborative ID framework for M2M based IoT, that leverages collaboration between IoT nodes for effective ID without consuming high communication, processing and energy resources. The proposed framework envisioned the collective use of the information from HIDS and NIDS. The proposed framework is planned to address challenges for example the flexibility, resource limitations of the nodes, and the collaborative nature of the M2M networks.

Table 4: Distributed and Centralized IDS advantages and disadvantages

IDS	Advantages	Disadvantages
Distributed IDS	▪ Flexibility and scalability. ▪ Detects DOS attacks for high-speed networks. ▪ Reduce computational costs. ▪ Monitoring, analysis, and processing of attack data is easier and speedier. ▪ Make possible an early intrusion detection that can result in blocking incoming traffic into the whole network from specific IP addresses.	▪ The data stream among the host and the agent may produce high network traffic overheads. ▪ The Data whose path is long from its source to the IDS potentially intercepted or modified which may result in misinterpretations. ▪ Can generate diverse outputs from different IDs.
Centralized IDS	▪ The maintenance and administration cost lower compared to the case of a distributed system. ▪ All of the IDS activities are controlled directly by a central console.	▪ Not able to detect malicious events occurring at different places at the same time. ▪ A hacker can incapacitate the programs running on a system, making the IDS unusable or unreliable.

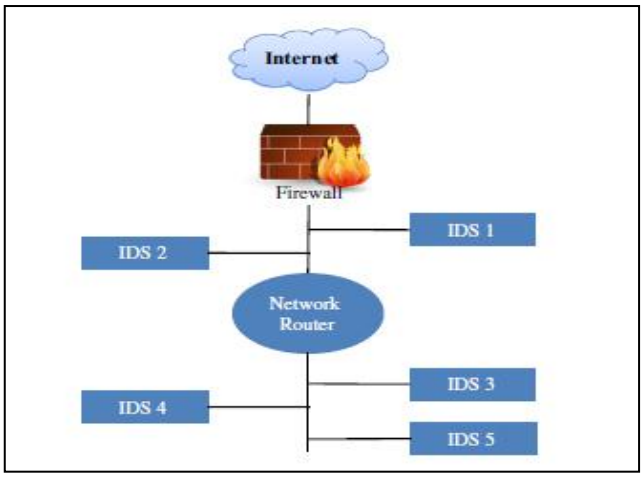

Figure 8: DIDS [12]

3.8 Database IDS

Database IDS monitors and checks attacks toward database. There are several types of database attacks such as SQL injection attack, Direct DB Attack [40]. Several researches addressed SQL injection attack, for instance: Liu A et al. [56] proposed SQL Proxy-based Blocker. In the SQLProb proposed method harnessed the Genetic Algorithms to dynamically detect and extract users entries for adverse SQL, and used a proxy that integrated with environment presenting protection to front-end web servers and back-end databases.

3.9 Hypervisor based IDS (Virtual Machine Introspection based IDS (VMI-IDS) Virtual IDS (V-IDS)

The concept of VMI was first introduced by Garfinkel et al. [57] as a hypervisor-level IDS which offered isolation for the IDS, while still offering visibility into the state of the host. VM-Based IDS is advanced based on three VM abilities: Isolation, Inspection, and Interposition [58].

Hypervisor is a platform runs VMs Hypervisor-based IDS which is working at hypervisor layer. It allows users to monitor and analyze connections among VMs or amongst hypervisor and VM and within the hypervisor based virtual network [12, 22]. It can preserve and apply diverse security strategies for each VM based on their requirements [22]. In Xen Hypervisor for example Openstack [59], VMI-IDS can be formed to run at the privilege domain of virtual machine monitor. The most important benefit of hypervisor-based IDS is an availability of information [12]. VMI-IDS observed hardware and software states and events of a host and offers the more strong view of the system than HIDS.

Figure 9 shows VMI-IDS architecture. VMI-IDS observes the programs running in VM to detect any abnormal activity [60]. There are many IDS in the cloud environment for example: The authors in [61] proposed novel classification of IDS in a cloud across deployment architecture and technique used. The IDS classification is shown in figure 10. It shows VM-IDS such as IDSaaS [62], VMM-based IDS such as VMfence [63]. Mishra et al. [34] proposed a Virtual Machine Introspection designed for fine granular monitoring of the VMs to detect attacks. The authors developed methods for monitoring and analyzing the Tenant Virtual Machines (TVM) at the process and system call level to detect attacks. In the proposed framework has been detected abnormal hidden processes, attacks that stop security tools in the VM also attack that alter the behavior of the authentic processes to access sensitive data. This proposed architecture named VMGuard utilized the introspection feature at the VMM-layer and to extract and select features the authors have been applied Bag of N-grams method combined with Term Frequency-Inverse Document Frequency technique, the authors then have been used the Random Forest classifier to introduced a common behavior for diverse classes of intrusions of TVM.

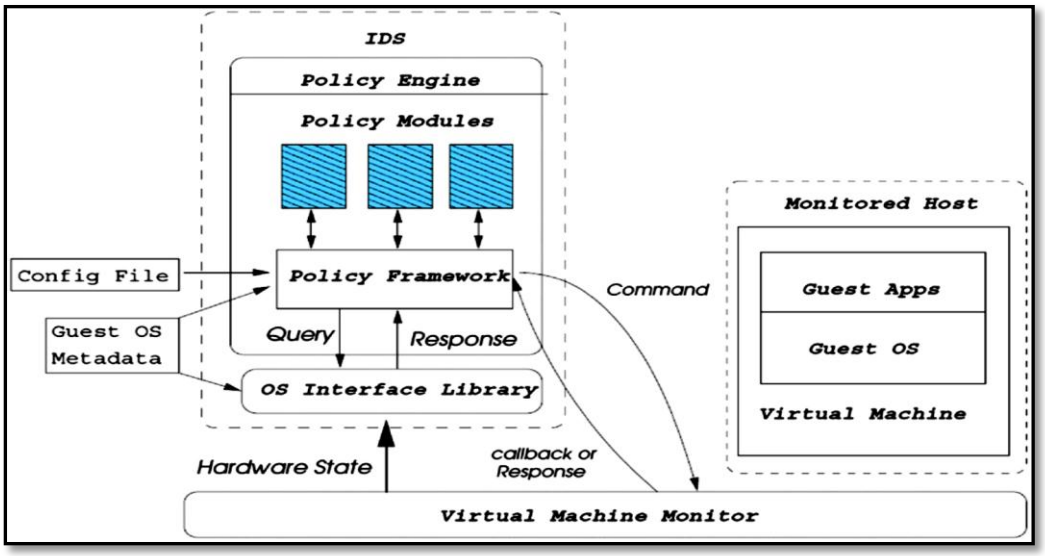

Figure 9: VMI-IDS architecture

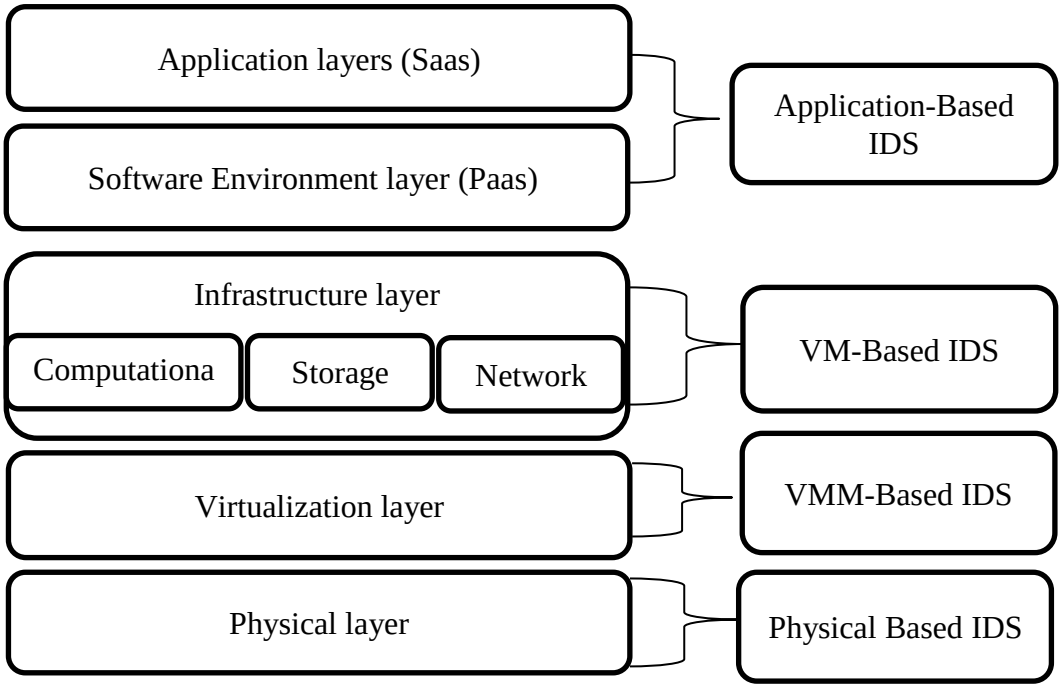

Figure 10: VM-IDS classification [61]

4 DISCUSSION

This paper is presented, based on first publications about IDS and focus on articles from 2008 until 2018 covered by journals and institutes such as: ELSEVIER Publishing company Journal, AMC, IEEE, Springer, SANS Institute and others. Many researches attempt to find effective tools for intrusion detection. The Developing effective tools based on the environment that deploys in it and the data that is analyzed to detect attack or intrusions. A summary of selected papers based on intrusion detection system type, platform, source of data, attack that detected are shown in table 6 order by publication year from newest to oldest. Table 1 displayed comparative between IDS types based on a platform that it deployed in it and data that input for analysis and what attack that can be detected. The platform is a host (single machine), network or hybrid on the host, and network or VM whether on host/network. Input data such as system event, traffic network and application activity. An attack that was detected can be classified as four classes according to the most of researches that used KDD dataset benchmark in IDS: Probe, Remote-to-Local (R2L) attack, User-to-Root (U2R), Denial-of-Service (DOS) attacks and a lot of other attacks which the researches detection.

When develop and use IDS the first thing you require to study the environment that wants to secure and select IDS based on the operating system and network topology. In section 3, the authors discussed different IDS types and introduced overview of it for help researcher to keep research time of IDS types and open new issues for new research to solve problems of any types. In this section, the authors display the advantages and the disadvantages of IDS types to provide a general overview of the features and disadvantages of each type and to identify leading trends, open issues, and future research possibilities. Figure 11 shows the percentage of covered papers in our work over publication years.

In table 5 has been summarized the advantages and disadvantages of IDS types for easy understanding, and help in select appropriate type. The result of the comparison between IDS types can help developer and researcher to develop appropriate type and tools for IDS based on the available infrastructure. From table 5 the authors make the following observations about development some IDS:

- HIDS Development when needed to detect attack after or before an attack happens, to secure host recourse also to install IDS on operating system (OS) without the need for any hardware.
- NIDS Development when needed for IDS independent of OS and to secure network and multi host, also to detect network attack that HIDS cannot detect it, some attack that NIDS can detect it displayed in table 1.
- WIDS Development when needed to use wireless network, needed to scalable IDS and to detect Packet drop attack and mobile attack.
- DIDS Development when needed to detect DDOS attack, to speed detect process. DIDS designed to operate in a heterogeneous environment and detect the malicious event occurring at different places at the same time.

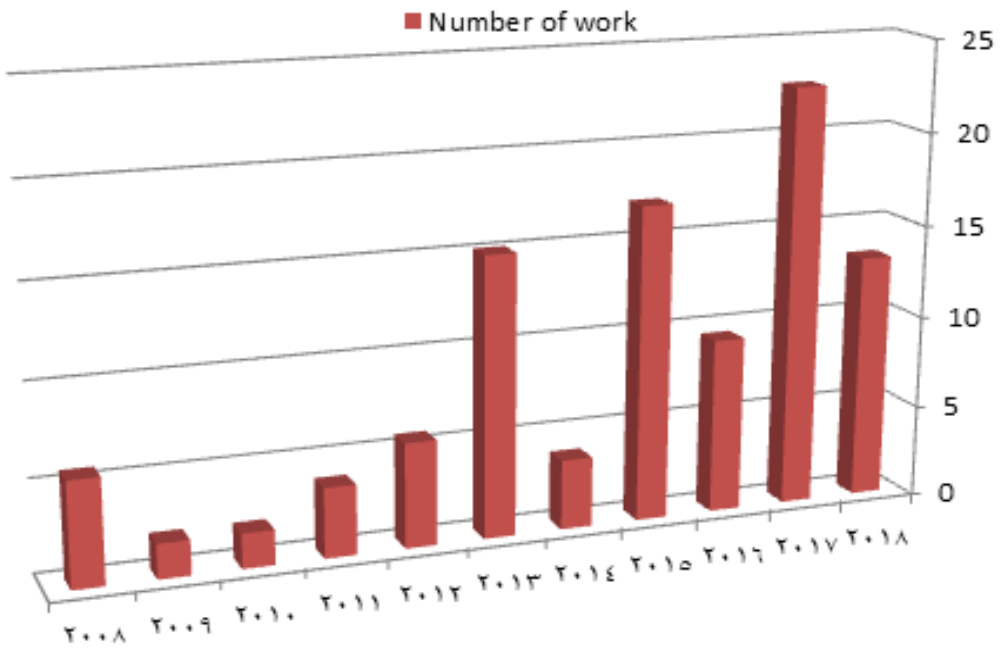

Figure 11: literature over years

Table 5: Advantages and disadvantages of IDS Type

IDS	Advantages	Disadvantages
HIDS	▪ HIDS can analyze encrypted data and communications activity. ▪ HIDS telling us if an attack is successful or no. ▪ Easy to deploy because it does not require additional hardware, therefore, it does not affect the current architecture.	▪ HIDS breakdown if the OS break down by the attack. ▪ HIDS are not able to detect network scans or DOS attack. ▪ HIDS tend to be resource intensive.
NIDS	▪ Operating Environment Independent, therefore NIDS will not affect the performances of hosts.	▪ Does not indicate whether the attack was successful or no. ▪ Cannot Analyze Encrypted Traffic. ▪ NIDS is has very limited visibility inside the host machine.
MIDS	▪ More flexible. ▪ More Efficient. ▪ MIDS take advantage of the strengths of the combined type.	▪ High overhead load on the monitored system depending on the combined methodologies. ▪ Processor utilization of the hybrid agent is much great.
WIDS	▪ More accurate. ▪ It can manage wireless protocol activity.	▪ Sensors has limited computational resource and limited energy [16].
PIDS and APIDS	▪ APIDS focus on observing and analyzing operations particular to the application. ▪ More easier to define the normal and the abnormal behavior.	▪ Larger system overhead. ▪ Specific development [64]. ▪ It does not detect attacks below the application layer.
NBA	▪ Superior detection reconnaissance scanning, reconstruct malware infections and DDoS attacks. ▪ Effective on detect zero day exploits or new attack that no have signature in IDS database.	▪ Delay in detecting attacks. ▪ Some attacks may not be detected until they have already damaged systems especially attacks that occur quickly.
DIDS	▪ More scalable than standalone IDSs [54]. ▪ Monitoring, analysis, and processing of attack data is easier and speed and lower cost.	▪ Produces a high false alarm rate. ▪ Can have diverse outputs from different IDS.
VMI-IDS	▪ Offers more robust view of the system. ▪ Preserve and apply different security strategies for each VM.	▪ Virtualization adds additional layers, which can increase the security management and controls overhead. ▪ Some virtualization systems make it easy to share information between the systems; this convenience can turn out to be an attack vector if it is not carefully controlled.

Table 6: Comparative of selected literature work

The work	Year Published	IDS type	Platform	Data source	Attack type that detected
[31]	2018	HIDS	Host	System call	Unknown attack
[34]	2018	VMI-IDS	VM	Process and system call	Abnormal hidden processes. Attacks that debilitate security facilities. Attacks that alter the behavior of the authentic processes.
[37]	2018	NIDS	Network	UDP and ICMP source bytes	DOS attack.
[38]	2018	NIDS	Network	Network traffic	Not specific.
[42]	2018	PIDS	Network	Real time network traffic	Jamming attacks.
[55]	2018	CIDS	Host and Network	Data collective from host and network	Not specific.
[32]	2017	HIDS	Host	System call	Intrusive process.
[39]	2017	NIDS	Network	Network traffic	DOS, Probe, R2L, U2R.
[48]	2017	WIDS	Network	Network traffic	Land, Neptune, pod, Smurf, Tear drop.
[49]	2017	WIDS	Network	Wireless traffic	Intrusive traces from a wireless.
[50]	2017	WIDS	Network	Wireless traffic	Spoofing attack.
[51]	2017	DIDS	Host and Network	Network traffic	TCP Flood Attack.
[53]	2017	DIDS	Host and Network	Network traffic	Attacks that try to fail communication between nodes.
[33]	2014	HIDS	Host	System call traces	Malicious activities within the system
[47]	2014	NBA	Network	Network traffic	Insider activities.
[63]	2013	VMM IDS	VM	Network flow and files	Intrusion network attack and not file integrity.
[45]	2011	NBA	Host and Network	Log network, user activity.	User's activities.
[24]	2010	HIDS	Host	Log files	Anomaly System Behavior.
[56]	2009	Database IDS	Host and Network	Proxy data. SQL query.	SQL injection attacks.

5 CONCLUSION AND FUTURE WORK

The IDS is one of amongst the most essential consideration of cyber-security that can discover intrusion before and/or after attack occur. It plays an important role as a defending mechanism of networks and systems. An ID monitors and analyses data in a system to detect any attack. Intrusion detection has improved dramatically over time, especially in the past few years due to the newly advanced technologies. This paper provided an overall review of IDS types that are deployed in various environments or platform and introduced comparative between them. It introduced their features, advantages and disadvantages of each type. Also, the authors introduced a classification of IDS types based on some criteria such as platform -network, host, virtual machine and hybrid- and input data. For future work, the authors proposed the framework for NIDS to addresses some disadvantages of it.

REFERENCES

1. Akbar, S., T.S. Rao, and M.A. Hussain, *A Hybrid Scheme based on Big Data Analytics using Intrusion Detection System.* Indian Journal of Science and Technology, 2016. **9**(33).
2. Anderson, J.P., *Computer security threat monitoring and surveillance*. 1980, Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.
3. Swathi Pai M., B.B.K., *Big Data Security Analytic: A classification*

technique for Intrusion Detection System. ResearchGate, 2015.

4. Ashoor, A.S. and S. Gore, *Importance of intrusion detection system (IDS).* International Journal of Scientific and Engineering Research, 2011. **2**(1): p. 1-4.
5. Soniya, S.S. and S.M.C. Vigila. *Intrusion detection system: Classification and techniques*. in *Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on*. 2016. IEEE.
6. A. K. Saxena, S.S.a.P.S., *General study of intrusion detection system and survey of agent based intrusion detection system,,* in *International Conference on Computing, Communication and Automation (ICCCA)*. 2017, IEEE: Greater Noida, India. p. 471-421.
7. Suramwar, M.V. and S. Bansode, *A Survey on different types of Intrusion Detection Systems.* International Journal of Computer Applications, 2015. **122**(16).
8. Liao, H.-J., et al., *Intrusion detection system: A comprehensive review.* Journal of Network and Computer Applications, 2013. **36**(1): p. 16-24.
9. Chiba, Z., et al. *A survey of intrusion detection systems for cloud computing environment*. in *Engineering & MIS (ICEMIS), International Conference on*. 2016. IEEE.
10. Zarpelão, B.B., et al., *A Survey of Intrusion Detection in I nternet of Things.* Journal of Network and Computer Applications, 2017.
11. Zuech, R., T.M. Khoshgoftaar, and R. Wald, *Intrusion detection and big heterogeneous data: a survey*. Journal of Big Data, 2015. **2**(1): p. 3.
12. Modi, C., et al., *A survey of intrusion detection techniques in cloud.* Journal of Network and Computer Applications, 2013. **36**(1): p. 42-57.
13. Latha, S. and S.J. Prakash. *A survey on network attacks and Intrusion detection systems*. in *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on*. 2017. IEEE.
14. Wu, M. *Protocol-based classification for intrusion detection*. in *WSEAS International Conference. Proceedings.*

Mathematics and Computers in Science and Engineering. 2008. World Scientific and Engineering Academy and Society.
15. Sengar, H., et al. *VoIP intrusion detection through interacting protocol state machines*. in *Dependable Systems and Networks, 2006. DSN 2006. International Conference on*. 2006. IEEE.
16. Can, O. and O.K. Sahingoz. *A survey of intrusion detection systems in wireless sensor networks*. in *Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on*. 2015. IEEE.
17. Farooqi, A.H. and F.A. Khan, *A survey of intrusion detection systems for wireless sensor networks.* International Journal of Ad Hoc and Ubiquitous Computing, 2012. **9**(2): p. 69-83.
18. Damshenas, M., A. Dehghantanha, and R. Mahmoud, *A survey on malware propagation, analysis, and detection.* International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2013. **2**(4): p. 10-29.
19. Snapp, S.R., et al. *DIDS (distributed intrusion detection system)-motivation, architecture, and an early prototype*. in *Proceedings of the 14th national computer security conference*. 1991. Washington, DC.
20. Folino, G. and P. Sabatino, *Ensemble based collaborative and distributed intrusion detection systems: A survey.* Journal of Network and Computer Applications, 2016. **66**: p. 1-16.
21. Shar, L.K. and H.B.K. Tan, *Defeating SQL injection.* Computer, 2013. **46**(3): p. 69-77.
22. Mishra, P., et al., *Intrusion detection techniques in cloud environment: A survey.* Journal of Network and Computer Applications, 2017. **77**: p. 18-47.
23. Modi, C.N. and K. Acha, *Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review.* the Journal of Supercomputing, 2017. **73**(3): p. 1192-1234.
24. Vokorokos, L. and A. Baláž. *Host-based intrusion detection system*. in *Intelligent Engineering Systems (INES), 2010 14th International Conference on*. 2010. IEEE.
25. Chauhan, P. and N. Chandra, *A Review on Hybrid Intrusion Detection System using Artificial Immune System Approaches.* International Journal of Computer Applications, 2013. **68**(20).
26. Sarmah, A., *Intrusion detection systems; definition, need and challenges*. 2001, October.
27. Consortium, I.D.S., *Intrusion Detection Systems buyers guide*. 1999, Technical report, ICSA .NET.
28. Kozushko, H., *Intrusion detection: Host-based and network-based intrusion detection systems.* Independent study, 2003.
29. Bray, R., D. Cid, and A. Hay, *OSSEC host-based intrusion detection guide*. 2008: Syngress.
30. Kim, G.H. and E.H. Spafford. *The design and implementation of tripwire: A file system integrity checker*. in *Proceedings of the 2nd ACM Conference on Computer and Communications Security*. 1994. ACM.
31. Marteau, P.-F., *Sequence covering for efficient host-based intrusion detection.* IEEE Transactions on Information Forensics and Security, 2018.
32. Subba, B., S. Biswas, and S. Karmakar. *Host based intrusion detection system using frequency analysis of n-gram terms*. in *Region 10 Conference, TENCON 2017-2017 IEEE*. 2017. IEEE.
33. Deshpande, P., et al., *HIDS: A host based intrusion detection system for cloud computing environment.* International Journal of System Assurance Engineering and Management, 2014: p. 1-10.
34. Mishra, P., et al., *VMGuard: A VMI-based Security Architecture for Intrusion Detection in Cloud Environment.* IEEE Transactions on Cloud Computing, 2018.
35. Roesch, M. *Snort: Lightweight intrusion detection for networks*. in *Lisa*. 1999.

36. Vigna, G. and R.A. Kemmerer. *NetSTAT: A network-based intrusion detection approach*. in *Computer Security Applications Conference, 1998. Proceedings. 14th Annual*. 1998. IEEE.
37. Sklavounos, D., A. Edoh, and G. Paraskevopoulos, *Utilization of Statistical Control Charts for DoS Network Intrusion Detection.* International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2018. **7**(2): p. 166-174.
38. Othman, S.M., et al., *Intrusion detection model using machine learning algorithm on Big Data environment.* Journal of Big Data, 2018. **5**(1): p. 34.
39. Parvat, A., et al. *Network Intrusion Detection System Using Ensemble of Binary Deep Learning Classifiers*. in *International Conference on Smart Trends for Information Technology and Computer Communications*. 2017. Springer.
40. Seethalakshmi, D. and G.M. Nasira. *Detecting and preventing intrusion in multi-tier web applications using double guard*. in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*. 2016.
41. Patel, A., et al., *An intrusion detection and prevention system in cloud computing: A systematic review.* Journal of network and computer applications, 2013. **36**(1): p. 25-41.
42. Danish, S.M., et al. *Network Intrusion Detection System for Jamming Attack in LoRaWAN Join Procedure*. in *2018 IEEE International Conference on Communications (ICC)*. 2018. IEEE.
43. Scarfone, K. and P. Mell, *Guide to intrusion detection and prevention systems (idps).* NIST special publication, 2007. **800**(2007): p. 94.
44. Sabahi, F. and A. Movaghar. *Intrusion detection: A survey*. in *Systems and Networks Communications, 2008. ICSNC'08. 3rd International Conference on*. 2008. IEEE.
45. Kakuru, S. *Behavior based network traffic analysis tool*. in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*. 2011. IEEE.
46. Nitin, T., S.R. Singh, and P.G. Singh, *Intrusion Detection and Prevention System (IDPS) Technology-Network Behavior Analysis System (NBAS).* ISCA J. Engineering Sci, 2012. **1**(1): p. 51-56.
47. Koch, R., M. Golling, and G.D. Rodosek, *Behavior-based intrusion detection in encrypted environments.* IEEE Communications Magazine, 2014. **52**(7): p. 124-131.
48. Devi, R., et al., *Implementation of intrusion detection system using adaptive neuro-fuzzy inference system for 5G wireless communication network.* AEU-International Journal of Electronics and Communications, 2017. **74**: p. 94-106.
49. Kolias, C., V. Kolias, and G. Kambourakis, *TermID: a distributed swarm intelligence-based approach for wireless intrusion detection.* International Journal of Information Security, 2017. **16**(4): p. 401-416.
50. Gupta, A., R.K. Jha, and S. Jain, *Attack modeling and intrusion detection system for 5G wireless communication network.* International Journal of Communication Systems, 2017. **30**(10): p. e3237.
51. Deepak, K., et al. *Distributed Intrusion Detection System for TCP Flood Attack*. in *Proceeding of International Conference on Intelligent Communication, Control and Devices*. 2017. Singapore: Springer Singapore.
52. Göcs, L. and Z.C. Johanyák, *SURVEY ON INTRUSION DETECTION SYSTEMS*, in *7th International Scientific and Expert Conference TEAM 2015 Technique, Education, Agriculture & Management*. 2015: Belgrade.
53. Khan, Z.A. and P. Herrmann. *A trust based distributed intrusion detection mechanism for internet of things*. in *Advanced Information Networking and Applications (AINA), 2017 IEEE 31st*

International Conference on. 2017. IEEE.
54. Vasilomanolakis, E., et al., *Taxonomy and survey of collaborative intrusion detection.* ACM Computing Surveys (CSUR), 2015. **47**(4): p. 55.
55. Arshad, J., et al., *A novel framework for collaborative intrusion detection for M2M networks.* International Conference on Information and Communication Systems (ICICS), IEEE, 2018.
56. Liu, A., et al. *SQLProb: a proxy-based architecture towards preventing SQL injection attacks*. in *Proceedings of the 2009 ACM symposium on Applied Computing*. 2009. ACM.
57. Garfinkel, T. and M. Rosenblum. *A Virtual Machine Introspection Based Architecture for Intrusion Detection*. in *Ndss*. 2003.
58. Martinez, P.S., *Virtual Machines and Security*. 2013.
59. https://www.openstack.org/software/. *OpenStack*. 2015.
60. Hebbal, Y., S. Laniepce, and J.-M. Menaud. *Virtual machine introspection: Techniques and applications*. in *Availability, Reliability and Security (ARES), 2015 10th International Conference on*. 2015. IEEE.
61. Elsayed, M. and M. Zulkernine, *A Classification of Intrusion Detection Systems in the Cloud.* Journal of Information Processing, 2015. **23**(4): p. 392-401.
62. Alharkan, T. and P. Martin. *IDSaaS: Intrusion detection system as a service in public clouds*. in *Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012)*. 2012. IEEE Computer Society.
63. Jin, H., et al., *A VMM-based intrusion prevention system in cloud computing environment.* The Journal of Supercomputing, 2013. **66**(3): p. 1133-1151.
64. Lazarevic, A., V. Kumar, and J. Srivastava, *Intrusion detection: A survey*, in *Managing Cyber Threats*. 2005, Springer. p. 19-78.