Wireless Networks (2021) 27:1269–1285
https://doi.org/10.1007/s11276-020-02529-3

Intrusion detection techniques in network environment: a systematic review

Maruthi Rohit Ayyagari[1] · Nishtha Kesswani[2] · Munish Kumar[3] · Krishan Kumar[4]

Accepted: 17 December 2020 / Published online: 2 January 2021

Abstract
The entire world relates to some network capabilities in some way or the other. The data transmission on the network is getting more straightforward and quicker. An intrusion detection system helps distinguish unauthorized activities or intrusions that may settle the confidentiality, integrity, or availability of a resource. Nowadays, almost all institutions are using network-related facilities like schools, banks, offices, etc. Social media has become so popular that nearly every individual belongs to a new nation called 'Netizen.' Several approaches have been implemented to incorporate security features in network-related issues. However, vulnerable attacks are continuous, so intrusion detection systems have been proposed to secure computer systems and networks. Network security is a piece of the most fundamental issues in Computer Network Management. Moreover, an intrusion is considered to be the most revealed dangers to security. With the evolution of the networks, intrusion detection has emerged as a crucial field in networks' security. The main aim of this article is to deliver a systematic review of intrusion detection approaches and systems that are used in various network environments.

Keywords HIDS · NIDS · Network security · Intrusion detection

1 Introduction

The internet and the related aspects are an ever-growing domain for research. As more and more services are available on the internet, so are threats and malware. Global digital has collected and synthesized data from various sources and published a report which revealed a massive hike in internet users for the year 2019. There is an increase of 366 million internet users that leads to 4.39 billion users in January 2019. There is a spiking growth of 9% in comparison to January 2018. In another report on malware, the centre for internet security revealed alarming data that showed an overall increase of 61% in malware activity in 2019. Figure 1 shows information regarding targeted attacks in the top 10 countries in the middle of the years 2015 and 2017. In the last decade, much advancement has been witnessed in the domain of attacks and anomaly detection. Any unwanted access to the system, using a malicious set of code aimed to exploit the system's weakness, is called an intrusion. An Intrusion detection system is software or hardware which detects malicious activity on a particular computer or a network. An IDS detects the vulnerability and alerts the system administrator for the same.

Intrusion detection systems are just like burglar alarms in the network whose role is to raise the alert to any malicious encounter in the system. It is the last resort where intrusion can be trapped before infecting the systems connected to the network for any network. Thus, Intrusion detection systems can be deployed at the network periphery or deployed at the host level. Intrusion Setection Systems (IDS) are the most important in-depth rooted devices in network security as they are deployed at the host levels.

✉ Munish Kumar
munishcse@gmail.com

[1] College of Business, University of Dallas, Irving, USA

[2] Department of Computer Science and Engineering, Central University of Rajasthan, Ajmer, Rajasthan, Punjab, India

[3] Department of Computational Sciences, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, India

[4] Department of Information Technology, University Institute of Engineering and Technology, Panjab University, Chandigarh, India

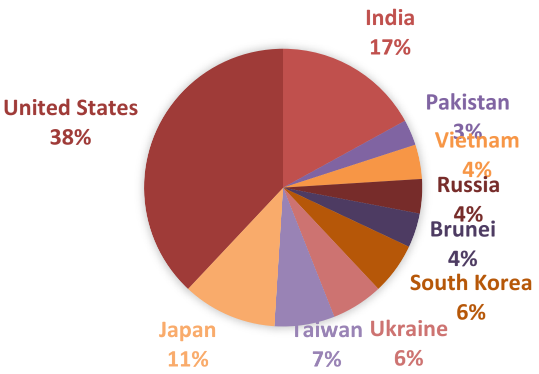


Fig. 1 Information regarding targeted attacks in the top 10 countries

Based on their deployment, they are classified viz. Network Intrusion Detection Systems (NIDS) and Host-Based Intrusion Detection Systems (HIDS) as shown in Fig. 2. Network Intrusion Detection System (NIDS) can use Signature or Anomaly methods to detect intrusions. Signature-based NIDS work on prior prepared patterns of known attacks, also called signatures. The benefit of a signature-based NIDS is its high accuracy in finding the known intrusions with low false alarm rates, but it is often criticized for detecting novel attacks. Further, the requirement for regular updating of the database makes it costlier and infeasible.

Anomaly-based NIDS deals with profiling user behavior. In this approach, an individual user normal activity model is defined, and any deviation from this model is known as anomalous. The benefit of an anomaly-based Network Intrusion Detection Systems is to predict novel attacks. Anomaly-based IDS are further classified as statistical IDS, knowledge-based IDS, and machine learning-based IDS. Machine learning techniques are resilient to noisy data and are robust and adaptable. Hence, most of the researchers are experimenting with these techniques. These have better performance due to low false alarm rates and a high detection rate compared to statistical and knowledge-based approaches. However, machine learning techniques suffer from the limitation of manual feature extraction. These may be inefficient to handle large amounts and various data, and sometimes, they cannot detect multi-classification attacks. In real-world applications, it is found that deep learning techniques may further improve accuracy with lower false alarm rates and higher detection rates. Fortunately, deep learning techniques are known for their ability to handle labeled or huge unlabeled data volumes. These techniques reduce the need for feature engineering, which is the most significant time-consuming part of machine learning.

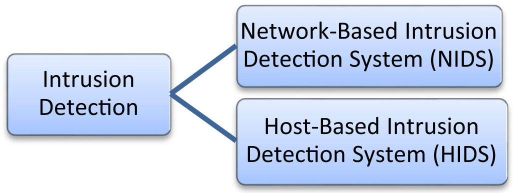

Intrusion Detection
Network-Based Intrusion Detection System (NIDS)
Host-Based Intrusion Detection System (HIDS)

Fig. 2 Types of intrusion detection systems based on their deployment

The deep learning system depends on the data patterns to detect human analysts' features would otherwise find it challenging to observe. Deployment of IDS and their use in the various network have been successful so far. In the past two decades, techniques for classification and detection of anomalies have undergone an enormous change. Earlier, intrusion detection was based on simple audit files of network data [50]. With the advent of new technologies, intrusion detection system has successfully detected attacks like Distributed Denial of Service (DDoS) attacks in the Cloud-based Networks [33] and black hole attack on Mobile ad-hoc Networks (MANETs). This motivated the researchers to review the various contemporary techniques implemented for intrusion detection. Table 1 represents different IDS techniques related to overhead communications and unfair load distribution.

Performance assessment of these IDS is a difficult chore due to various reasons that are given below. It is extremely difficult to get high-quality information for presenting the assessment because of security and other issues mentioned below:

- In real-time data, marking network connection as ordinary or intrusions need a lot of time.
- Continuous alteration of network traffic.
- Complexity in estimating the detection rate.
- Address the problem of a high false alarm rate.
- Different types of attacks.

1.1 Uniqueness and novelty of this article

This article presents a systematic and comprehensive survey for intrusion detection techniques. It has been observed from the previous survey articles that some research articles cover the background and the introductory part of the intrusion detection techniques. Other articles aim at the comparison of existing methods, but the analytical synthesis is missing. This article aims to present a complete guide about the introduction, need, fundamentals, types, characteristics, framework, and latest contributions for intrusion detection in network security. The intent is to inculcate curiosity for future research possibilities and ignite and motivate the readers for innovative developments and successful research.

Table 1 Various types of intrusion detection techniques

Intrusion detection system	Research	Overhead	Distribution of Load
Fuzzy C-means clustering	Hore et al. [16]	Pre-defined feature sets are extracted from packets and are exchanged	N/A
Self-organizing maps and wavelets	Li et al. [23]	The base station acquires full data records	N/A
Multi-agent and clustering based IDS	Guan and Truk [18]	All the records are exchanged across the nodes	N/A
Agglomerative clustering	Tan et al. [48]	Summaries of clustering are exchanged	N/A
Genetic algorithm and Deep Belief network	Zhang et al. [53]	GA detects the optimum number of hidden layers and nodes	GA increases the overhead on the nodes
Cluster-based IDS	Choudhary and Kesswani [9]	The cluster heads are responsible for intrusion detection	Cluster head is overloaded
Outlier-based IDS	Verma and Ranga [51]	Copycat attack is detected using outliers	Outlier detection increase overhead on the nodes
Hierarchical IDS	Chang et al. [7]	Local and global anomaly detection	The load is distributed across the hierarchy

2 Organization of the survey

The current survey helps beginner researchers gain insights into Intrusion Detection Systems and provide an overview of legitimate traffic and attacks. This section outlines basic ideas like planning, the research questions that it tries to address, the study bases, assessment of the quality, dataset sources, criteria for inclusion and exclusion of the existing research, and data pulling out techniques. In addition to this, the survey also highlights the demand of the system that has been studied, how it is accomplished, and in which domains it is beneficial. Furthermore, this survey explores the direction related to the cost, including resource and computational cost, data collection techniques, management of data, analysis, and recording of the results.

2.1 Planning the survey

The current survey design starts with reason and explanation behind the IDS investigation. The study's accomplishment relies upon the technique for introducing the motivation behind the review, objectives of the study, the construction of questions, and other pertinent specifics. The survey's planning phase reveals the methods that aid in moving towards the goal, criteria for inclusion and exclusion of the existing research, and assessment of IDS' experimental results.

2.2 Research questions

The research questions define the problems to be addressed by the current research. Table 2 tabulates the research questions related to IDS.

2.3 Inclusion and exclusion criteria

In all 70 articles were examined in the first stage based on the criteria for inclusion and exclusion of the existing research. In the second stage, 08 articles were excluded from the study; after that, in the third stage, 06 articles were excluded. Thus, after removal of duplicates, 56 publications were taken in the current study.

3 Types of intrusion detection systems

IDS can be classified on the basis of the method used for the detection of intrusions, the reaction of an IDS to detect an intrusion, or data collection, as depicted in Fig. 3.

3.1 Detection methods of IDS

The intrusion detection systems can be broadly divided into two categories based on the method used for detecting intrusions: Misuse Detection and Anomaly Detection.

3.1.1 Misuse detection

Misuse detection operates with ready-to-use templates of known attacks, also called signatures [37]. Stateless misuse detection systems use just the existing signatures, whereas stateful misuse detection systems use previous signatures too. The approach has been used widely because of high accuracy to find known intrusions with low false alarm rates but criticized for incapability to detect novel attacks, one of the solutions to address this problem is to regularly update the database which is infeasible and costly [41].

Table 2 Research objectives and motivations

Research questions	Remarks
What is an IDS	An Intrusion Detection System (IDS) is a software or hardware that monitors the network traffic to detect malicious activity and generates alerts if any such event is detected
Types of IDS	Host-based IDS deployed on the host and network-based IDS deployed on the network
The function of an IDS	An IDS detects malicious activity and generates an alarm
Challenges of managing an IDS	False-positive, staffing, missing a legitimate risk. There is a challenge if the traffic is encrypted
Future of IDS	Some researchers are also trying to design Intrusion Prevention Systems that work proactively

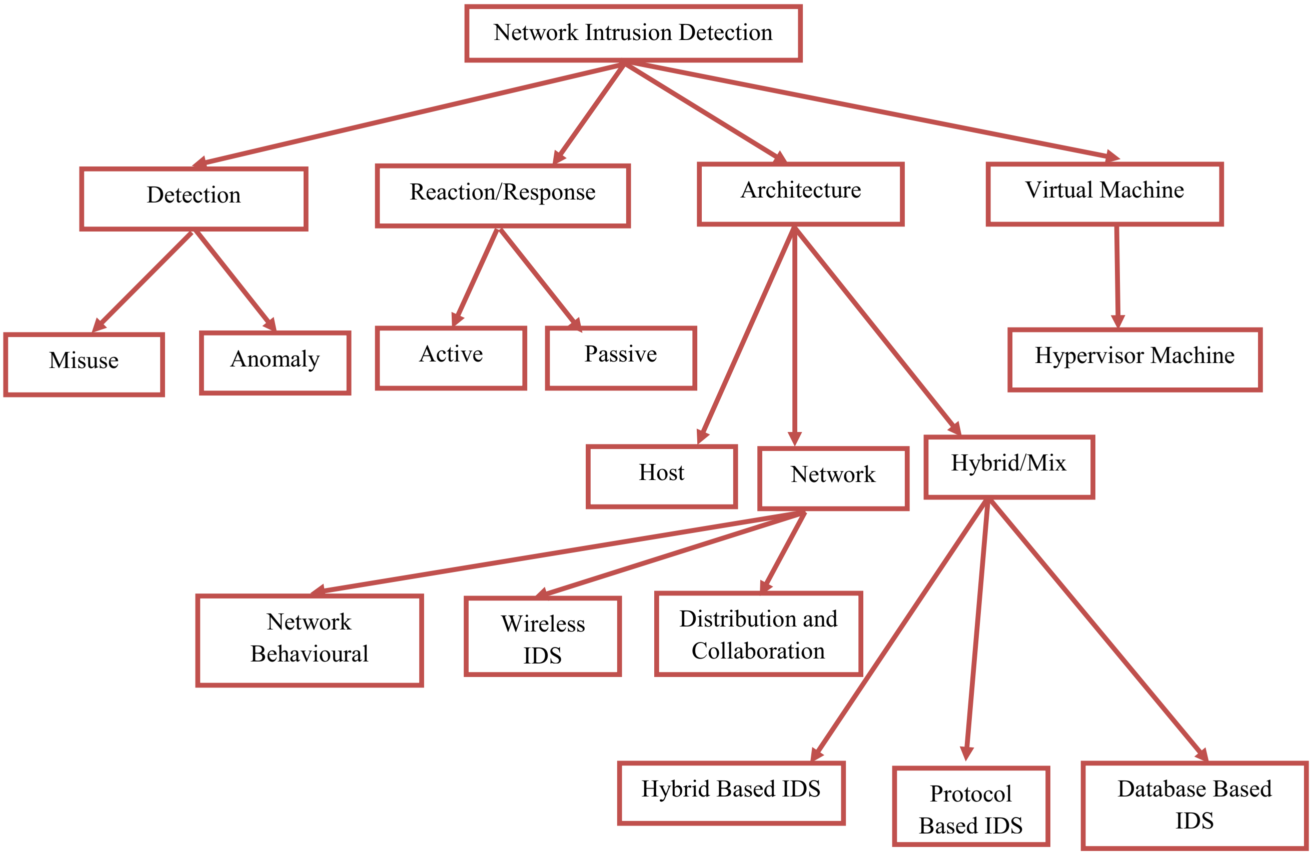


Fig. 3 Various categories of intrusion detection systems

Therefore, anomaly detection techniques came into existence. Anomaly detection deals with profiling user behavior (https://www.elprocus.com/basic-intrusion-detection-system/). In this approach, an individual user's regular activity model is defined, and any nonconformity from this model is known as anomalous. Anomaly detection methods are further categorized into two parts: static anomaly detection and dynamic anomaly detection. Static anomaly detection is based on a principle that only a fixed part of the system is scrutinized like operating system software, whereas dynamic anomaly detection extracts patterns (sometimes called profiles) from network usage history. It sets an edge to isolate ordinary usage from anomalous usage of resources. This strategy can identify attacks but may prompt a high false alarm rate and need high precision. An additional shortcoming is that if an attacker comes to know that the attacker is being profiled, he can gradually alter the profile to pretend the intruder's malicious behavior as normal [29].

3.1.2 Anomaly detection

The network traffic is monitored regularly and compared with the known behavior (Fig. 4). In the event of any

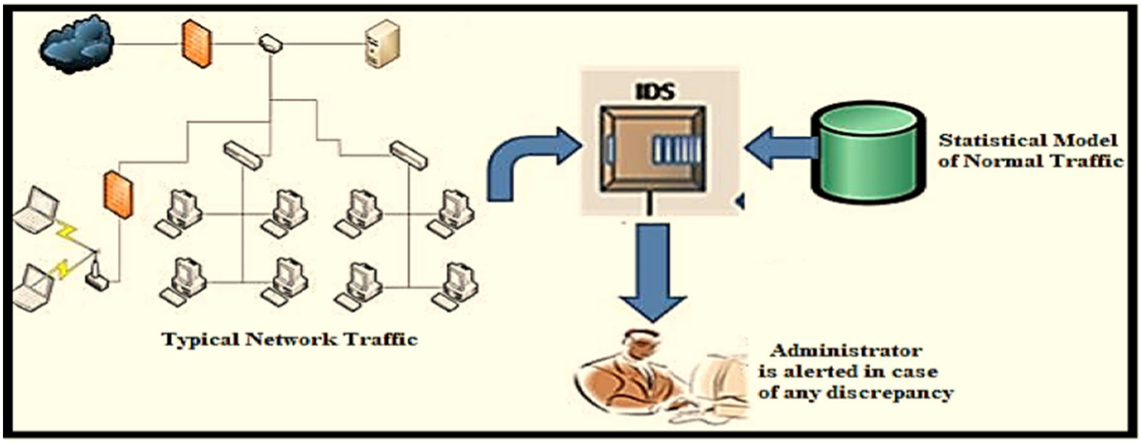

IDS
Statistical Model of Normal Traffic
Typical Network Traffic
Administrator is alerted in case of any discrepancy

Fig. 4 Anomaly-based intrusion detection system (Visit https://www.elprocus.com/basic-intrusion-detection-system/)

anomaly, it sends an alert. Anomaly-based IDS can detect new as well as unique attacks, it must be considered as an advantage of this system.

Anomaly detection based IDS are better as compared to misuse detection as no prior knowledge of attacks is required, and this method can detect unseen attacks as well.

3.2 Reaction/response methods of IDS

The reaction module's main objective is to trace back i.e. to determine the sequence of routers used by the attacker. Intrusions identified in such a manner by the detection module will trigger the subsequent reaction phase events. All the network routers cooperate to go as close as possible to the attack sources and set the most applicable countermeasures in an intrusion detection module. IDS can be categorized as passive or active. The detailed flow for passive IDS is described in Fig. 5.

One limitation of PIDS is that it merely alerts the system or network administrator and recognizes malware operation. Then, the administrator is required to take the necessary action.

3.3 Different architectures for IDS

The computer systems and networks handle various vulnerable user data that are vulnerable to different attacks from both interior and outer intruders [35]. For instance, Yahoo's data breach resulted in a loss of $350 Million, and the breach in Bitcoin caused a loss of $70Million [22]. Such kinds of cyber-attacks are continually advancing due to complex algorithms and progression of equipment, programming, and system configurations, including the recent improvements in the Internet of Things [50]. Malicious attacks present genuine security concerns that lead to the necessity for innovative, adaptable, and more dependable IDS. IDS should be capable of proactively detecting an intrusion. It should also detect and prevent intrusions, different types of attacks, or breach at the network-level or host-level effectively. Intrusion detection systems are categorized into network-based and host-based IDS [33].

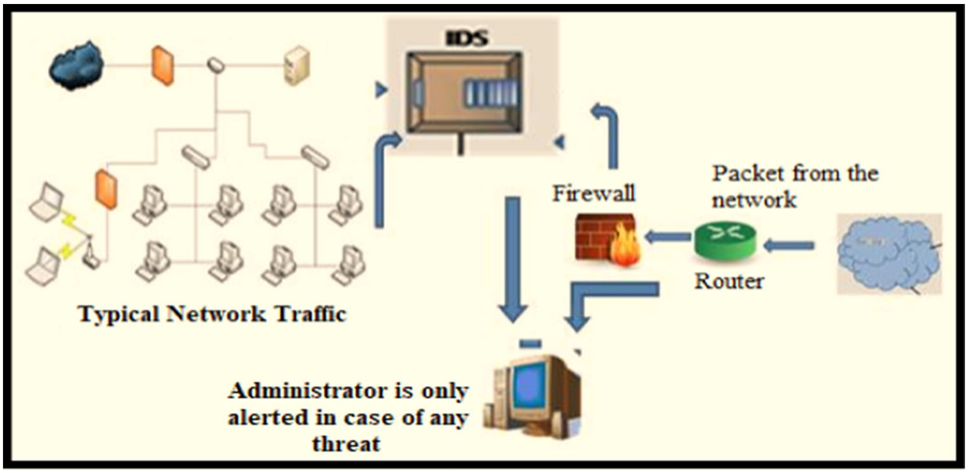


Fig. 5 Passive intrusion detection system (https://www.elprocus.com/basic-intrusion-detection-system/)

IDS can be deployed on the host, on the network, or both (host and network), i.e., hybrid. But it may be a costly option which might be unacceptable for customers running computationally greedy applications. Network-based IDS offer a different approach. They are extremely portable and are independent of the operating systems and only monitor traffic over a specific network segment. All attacks will be listening by deployed network-based intrusion detection sensors, in any case of the destination operating system type. The network-based solutions cannot keep up with heavy traffic; however, easier to implement. A system that unites both host and network-based characteristics appears like the most logical approach intuitively known as the hybrid approach.

3.3.1 Host based IDS

Host-based IDS can track the attributes and events related to an individual host. The HIDS has been established for hosts to assure continuous monitoring of the system. These systems often use information associated with the operating system of the target machines. System logs, file access, and modification, incoming and outgoing packets, currently executing processes, and HIDS monitor any other configuration changes. Intrusion can be reported by writing logs, sending e-mails, etc. in host-based IDS. The database is used to store objects and attributes [5]. HIDS is also known as System Integrity Verifier as it provides exhaustive information about the attack. One of the limitations of HIDS is that if a host is down due to attack, then HIDS is also down.

Further, it requires to be installed on the host; even the resources of the host are utilized. Despite this fact, HIDS overweighs NIDS in detecting malicious activities for a sole host. Popular products of HIDS are eXpert-BSM (Basic Security Module), Emerald, Dragon Squire, Intruder Alert, NFR (Network Flight Recorder), Host Intrusion Detection, and Snort.

3.3.2 Network IDS

An individual network's or subnet's traffic is checked in NIDS by continuously analyzing the traffic and comparing it with the attacks already available in the library. An alert is sent if an attack has been detected. Primarily, to monitor the network traffic, it is being deployed at an essential point in the network. It is usually placed between the network and the server or along with the network boundary. This system's main aim is that it can be deployed quickly at a lower cost without having it for each system, as shown in Fig. 6. It fundamentally focuses on detecting different types of intrusions like computer tampering, the existence of malware, and malicious activities. The major limitation of NIDS is that attack is undetectable if it is within the firewall perimeter. It works like anti-virus for the host when each network entity is interfaced with inbuilt NIDS. It can also decouple the host's operating system [52], which is termed as the main benefit of NIDS. Signature-based detection and anomaly-based NIDS are the two modern approaches for spotting attackers across the network [43].

The Network Behaviour Analysis (NBA) system researches the system traffic to recognize attacks with sudden traffic streams [26]. It watches and checks the network traffic to predict threats that lead to extraordinary streams, like DDOS attacks, the existence of viruses, and policy violations [37] and [41]. NBA-IDS is the most frequently deployed IDS on internal systems of an association. Sometimes, they can be deployed where the streams between an association's system and external systems can be screened [36].

a. Wireless IDS

A wireless intrusion detection system examines and evaluates remote traffic to identify any attacks [26]. There are various kinds of attacks on a wireless network such as sinkhole, black hole, wormhole, spoofing, flooding, cloneID, and Sybil attack. Figure 7 depicts the wireless intrusion detection system.

b. Distributed IDS

Distributed IDS is made up of multiple IDS distributed across a network. These IDS can connect or a server that monitors the system [34]. Figure 8 demonstrates distributed and collaborative IDS. Distributed IDS is intended to operate in a non-homogenous condition, which implies that DIDS analyzes real data from various sources to detect attacks such as a doorknob or DDoS attack. In a DIDS, the information studied might be proportionate to the number of hosts that are being checked.

c. Collaborative IDS

Collaborative IDS can associate cautions originating from differing sensors. These intrusions alarms are joined with the connection unit, then the reports are delivered, and the attack is confirmed [12]. There is a possibility to make the Intrusion Detection System independent, self-altering, parallel, organized, and efficient using CIDS. Isolated Intrusion Detection systems may not have the option to accomplish the association between malicious activities occurring at different places simultaneously [49].

d. Hybrid IDS

Hybrid IDS or mixed IDS is a combination of two or more types or IDS to leverage their advantages to achieve accurate detection. For example, a double guard uses host

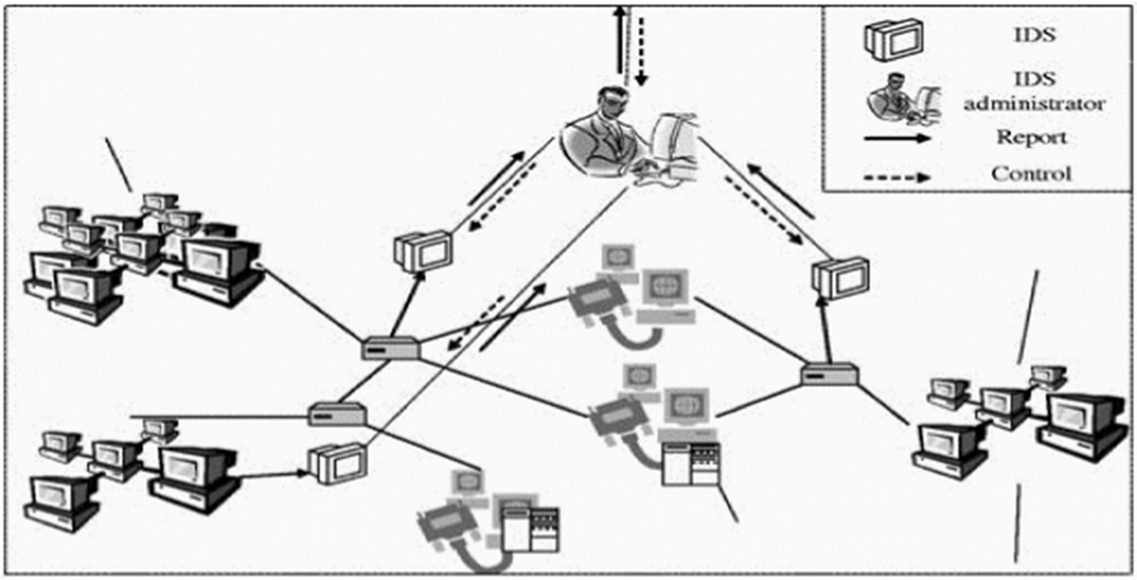
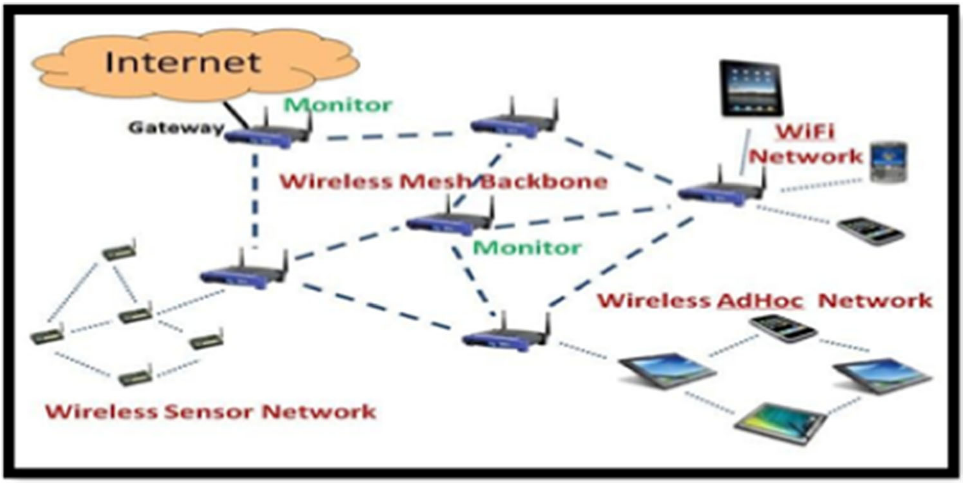


Fig. 6 Network intrusion detection system

Fig. 7 Wireless intrusion detection system



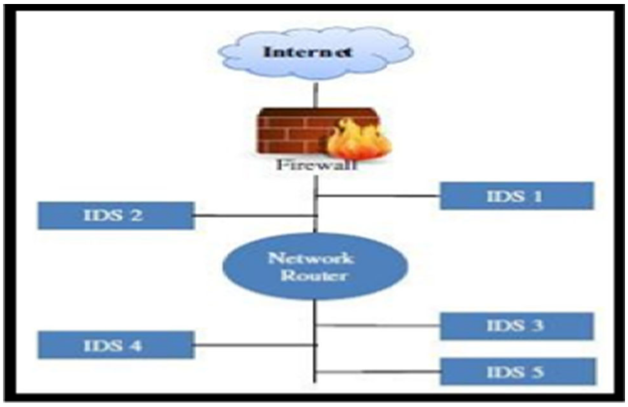


Fig. 8 Distributed and collaborative IDS

IDS and network IDS [26]. However, the Mixed intrusion Detection System takes longer to analyze the data. Figure 9 represents the Hybrid IDS.

e. Protocol Based IDS

Protocol-based IDS screens and checks the protocol's performance and the corresponding state like HyperText Transfer Protocol (HTTP) [54]. Protocol-based IDS can be specific to screen an application protocol, like APIDS (Access point intrusion detection system) [54]. PIDS centers on activities that occur in specific applications by observing and dissecting the application log documents or estimating their performance [38]. Danish et al. [10] suggested an Intrusion Detection System to recognize attacks in a Low Range Wide Area Network (LoRaWAN), a MAC protocol for Wide Area Networks.

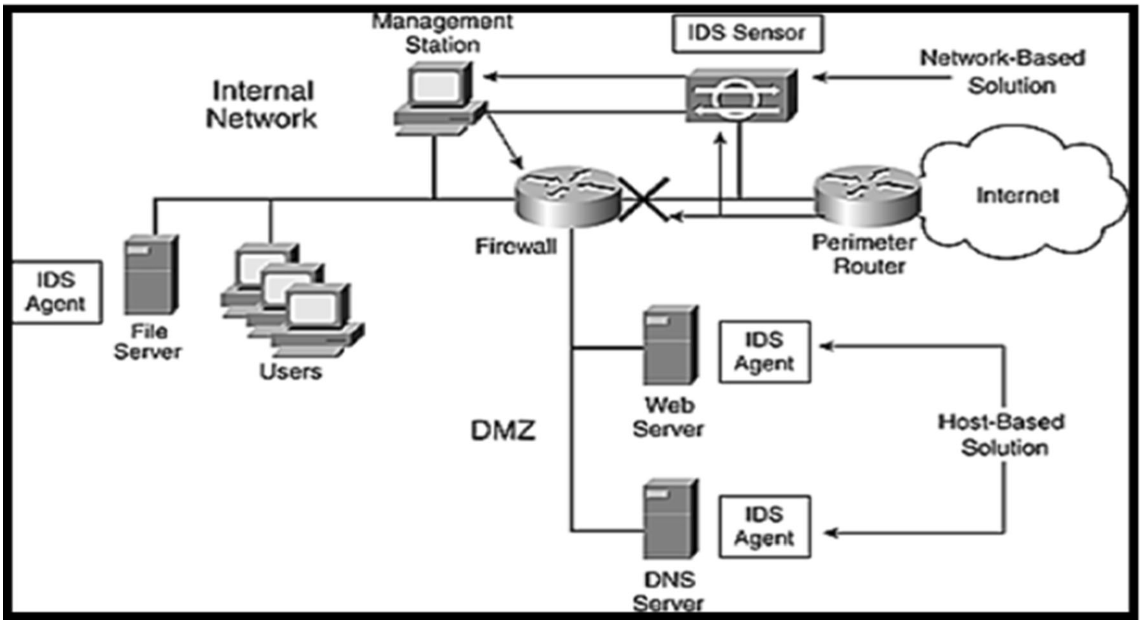


Fig. 9 Hybrid IDS

f. Database Based IDS

Database intrusion detection system screens, and checks attack on the database. The database attacks are of different types, for example, SQL (Structured Query Language) injection attack, Direct DB Attack [42], etc. Several studies had tried to address the SQL injection attack. One such study conducted by Liu et al. [29] recommended SQL Proxy-based Blocker for SQL injection attack. The proposed SQLProb used the Genetic Algorithms (GA) to powerfully distinguish and infer client's entrances for unfriendly SQL and used a proxy that helped introduce security on front-end web servers the databases at the back-end.

3.4 Virtual machine

The idea of Virtual Machine Introspection was presented by Garfinkel and Rosenblum [13] as hypervisor-level Intrusion Detection System helped incorporate isolation in the IDS, and at the same time, offers visibility into the state of the host machine. The procedure facilitates the construction of a Virtual Machine Introspection IDS is the virtual machine monitor (VMM). It is a piece of software that virtualizes the hardware located on a physical machine. It also partitions the physical Machine into logical virtual machines [13]. Figure 10 shows Virtual Machine Introspection based IDS (VMI-IDS) architecture. Virtual Machine Introspection based IDS (VMI-IDS) notices the processes running on Virtual Machine to notice any abnormal behavior [15].

The intrusion detection system classification is exhibited in Fig. 11. It illustrates Virtual Machine Intrusion Detection System such as IDSaaS [3], VMM-based Intrusion Detection System such as VMfence [17].

3.5 Features of IDS

Efficient IDS ought to have the following features:

- IDS should not behave like "black-box". The functionalities of the IDS should be reasonable for outcasts.
- IDS must be resilient to faults. It must be able to recover from a system crash.
- IDS must be capable of screening itself and returning back to a stable state.
- IDS should be able to run reliably without human intervention.
- IDS should not impose much overhead on the system resources.
- With changes in the system's behavior and advancements in the technologies, the IDS should be able to acclimatize.
- IDS must have the option to watch significant deviations from average system behavior.

Depending upon the requirement, different IDS architectures are used in different scenarios. Like Virtual Machine IDS is more appropriate for cloud-based environments. Similarly distributed IDS are more appropriate when the computers are distributed at various locations. The advantages and disadvantages of different IDS systems are presented in Table 3.

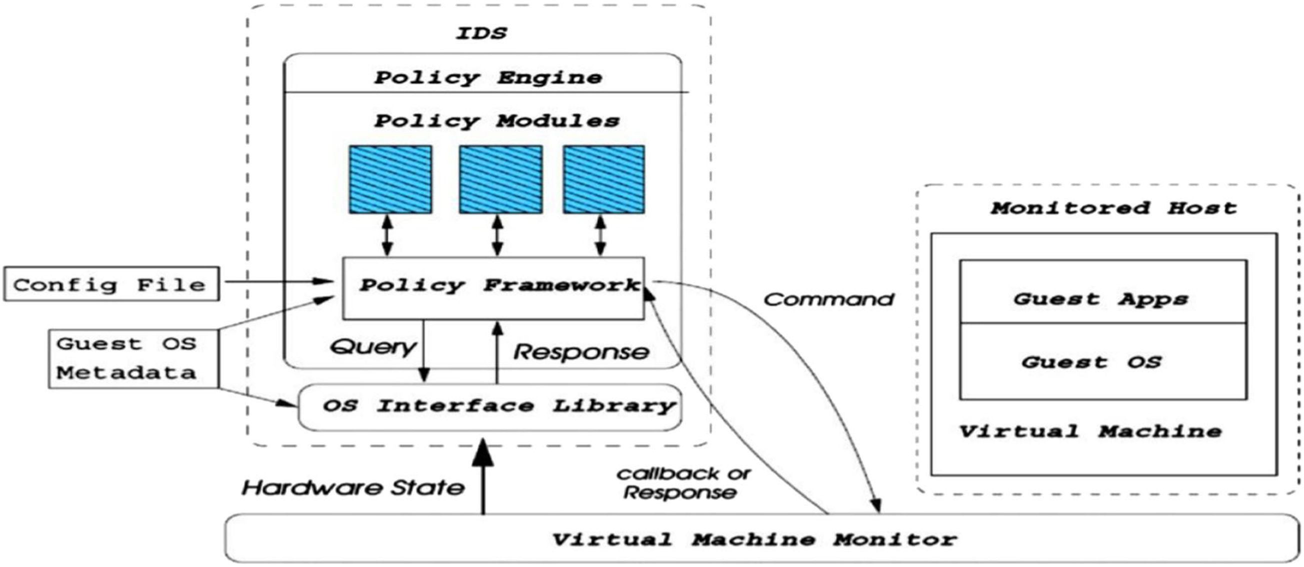
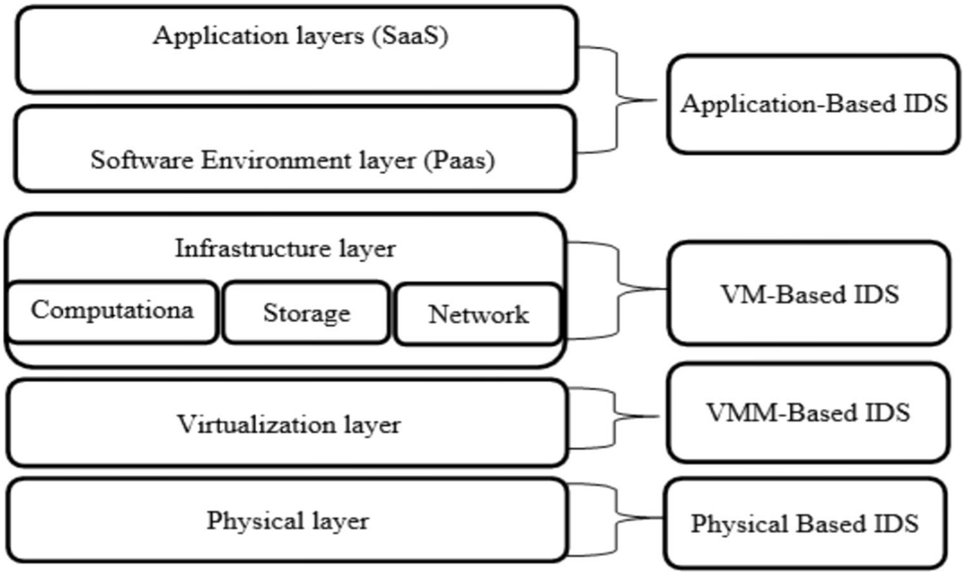


Fig. 10 Virtual machine introspection based IDS (VMI-IDS) architecture

Fig. 11 Virtual machine intrusion detection system classification



3.6 Datasets, network sniffers, and open-source NIDS

This section briefly illustrates the datasets and open-source network sniffers for IDS. Some of the datasets commonly used for intrusion detection in literature are KDD99, NSL-KDD, a modified version of KDD 99, UNSW-NB15, CICIDS, and CSE-CIC-IDS2018. KDD 99 and NSL-KDD focus on attacks like Denial of Service, Remote to User User to Root (U2R), and probing. In UNSW-NB15, there are nine types of attacks, including backdoors, DoS, generic, exploits, fuzzers, shellcode, worms, and reconnaissance. The attacks targeted in the CICIDS data set include FTP, brute force, DoS, DDoS, SSH, Heartbleed, web attack, botnet, and infiltration. Attacks included in CSE-CIC-IDS2018 are heartbleed, brute force, DoS, DDoS, web attacks, and botnets. The commonly used open-source network sniffers used for intrusion detection include Tcp-dump, Wireshark, Ettercap, Argus, EtherApe. There are several open-source NIDS, including Snort, Suricate, which is a signature-based IDS, Bro-IDS, Kismetm OpenWIPS, Onion Security, and Sagan.

4 Reported work for host and network IDS

This section presents the Intrusion Detection Systems based on Host and network-based Systems.

Table 3 Advantages and disadvantages of IDS

Intrusion detection system	Advantages	Disadvantages
Network intrusion detection system	Operating Environment NIDS does not impact the functionality of the hosts	Has limited visibility in the host machine Does not alarm if the attack was successful It is unable to analyze the encrypted traffic
Wireless intrusion detection system	WIDS can manage wireless protocol activity More accurate	Resource and limited energy Sensors have limited computational
Host intrusion detection system	Can also analyze encrypted data and communications Indicates if an attack is successful or not Does not require additional hardware and thus it is easy to deploy	In case the Operating System crashes due to an attack, HIDS stops functioning Tends to be resource-intensive Network scans or DOS attacks are difficult to detect
Mixed intrusion detection system	More Efficient More flexible MIDS takes advantage of the strength of the combined type.	High overhead on the monitored system as several techniques are combined CPU utilization is more
Protocol based IDS and Access Point IDS	Useful for specific applications Can easily segregate normal and abnormal behavior	Larger system overhead Not applicable to attacks on layers below the application layer Specific development
Database IDS	Easy to Monitor, analyze, and process attack data Higher speed and lower cost More scalable than standalone IDSs [49]	Produce a high false alarm rate Gives different results for different IDS
Virtual Machine Introspection based IDS	Offers a robust perspective of the IDS Distinctive security methodologies for every VM	Virtualization includes extra layers, that build the security Some of the virtualization frameworks can share data between the frameworks; this accommodation can end up being an assault vector if it isn't painstakingly controlled

4.1 Host based IDS

The main aim of HIDS is to control the behavior and dynamic state of the computer system. The flow of packets and all the activities on a network has been scrutinized by HIDS. The system administrators receive some network alerts if any alternation or adjustment happens in the network. HIDS is gradually becoming crucial in securing a host computer framework and its network. HIDS is incorporated into the computer system to identify the intruder's abnormal behavior. It also protects the information from intruders, and the incidents are reported to the system administrator. If an attack happens on any other part of the network, then host-based IDS will not only detect an attack, but it will also monitor incoming and outgoing traffic. The file system located on the host performs audits of the users' login, currently, active processes, resource utilization, and much more can also be analyzed by a host-based IDS. Following are some of the advantages of HIDS:

- All users' activities can be monitored in HIDS, whereas it is not conceivable in a network-based system.
- An attack that has been originated from the host side can be identified by HIDS.
- The decrypted traffic to find a host-based system can analyze an attack signature. Thus, they also have the capability of monitoring encrypted traffic.
- No extra hardware is required as they can be easily installed on the existing host devices.
- For a small-scale network, Host-based IDS is cost-effective.

Some of the disadvantages include that it may become problematic if the host device is compromised. Besides, it is extra computational overhead on the host on which IDS is located. In the case of attacks such as the denial of service (DoS), HIDS can be ineffective. PortSentry (https://securitywing.com/host-based-ids-vs-network-based-ids/) is an example of HIDS.

Taking the above into consideration, it is implied that there is no candid way to resolve which type of intrusion detection system will be paramount for the network as both the IDS have their advantages and disadvantages. A combination of both the IDS can be deployed, as network-based IDS provides security to the network, whereas HIDS will protect sensitive data on a host. Software applications (agents) and HIDS are installed on the computer systems that need to be monitored. The operating system is to be monitored by the agents and the data is written to the logs and alarms are triggered. The individual computer systems on which the agents are mounted can only be monitored by a host intrusion detection system, and the entire network cannot be monitored. Host-based IDS are helpful in monitoring intrusion attempts on critical servers.

An IDS based on statistical profiling is presented by Shavlik and Shavlik 44]. Measurements from 200 systems with Windows2000 have been taken to generate around 1500 features. The features that have been included are CPU utilization, information about processes, the quantity of data input and output, and differences and averages of present and historical values. The behavior of the users is accurately identified with the help of features and their associated weights. Furthermore, unique signatures have been created by assigning feature weights for each individual user.

A survey of Intrusion detection systems has been provided by Sabahi and Movaghar [41]. Various IDS techniques like Network IDS, DIDS, and Host IDS have been discussed in the survey. Along with this, detection methods like protocol analysis, misuse based, and anomaly detection have been illustrated in the study. Online and offline modes of detection on centralized and distributed architectures have been mentioned in the survey. Lin et al. [28] proposed Host-based IDS, which is an amalgam of misuse detection as well as supervised learning. Misuse detection is realized with the help of OSSEC, which is an open-source Intrusion Detection System. It is capable of analyzing the log files. Back Propagation Neural Network (BPNN) has been used for anomaly detection. For misuse detection, the log data has been collected, pre-processed, and analyzed using OSSEC, and finally, the results have been reported. Since HIDS can detect intrusion only on the host, the proposed approach has limited contribution. Moreover, it uses misuse based detection which is unable to detect new attacks.

Wu and Banzhaf [52] proposed a centralized Host-based IDS architecture for private cloud computing environments. The primary goal of the IDS is to minimize the usage of the resources of the system. The proposed model is assembled on OpenStack4, which is an open source platform. It is comprised of three nodes, i.e. compute, controller, and network nodes, and four modules for data collection, pre-processing of data, IDS detection, and alarm modules. The data collection module utilizes Log stash5 for the collection of logs from all the Virtual Machines and stocks it in the Elastic search6 for further analysis that is done by the detection module. The detection module is based on C5.0 decision tree. In case of an anomalous activity, the detection module alerts the victim Virtual Machine. The model was verified on KDD99 dataset and compared to a conventional HIDS. The results indicate that in the proposed HIDS CPU utilization is 14% less, memory usage is approximately 2% less, while detection rate is almost the same as the conventional HIDS which is 94%, and the detection time is slightly more. But in the proposed approach, since the IDS is centralized, it increases the overhead on the host machine,

Stavroulakis and Stamp [46] suggested classification of IDS approaches into three sub-categories i.e. computation intensive approaches, artificial intelligence based approaches, and biological concepts. Though, this classification does not cover all the properties of detection approaches, but such a classification is apt in the current scenario as artificial intelligence based approaches including machine learning approaches are known to give good accuracy. A HIDS screens and accumulates the features of hosts that contain sensitive data, servers, and other anomalous activities. A Network Intrusion Detection System monitors the network packets with the help of sensors, and further recognizes suspicious incidents by analyzing the activities across the network. Wireless Intrusion Detection Systems are like NIDS, but they capture the network traffic of wireless networks, like ad-hoc mesh and sensor networks. Adoption of multiple technologies like MIDS can help in more accurate detection. To avert the implementation of malicious code on the host machine, HIDS observers the logs of the system. But the implementation of HIDS is very challenging because of high false alarm rate in the case of HIDS. To reduce the problems like false alarm rates, semantic approaches have been used in this article. In the article, the semantic approach has been applied on the operating system calls to detect anomalous behavior. ADFA-LD dataset has been used to apply a semantic approach in order to detect intrusion on the host. ELM, The decision engine used in the research is capable of high learning speed at the same time it needs to be trained only once. But the overhead of processing time is more. Host Intrusion Detection Systems (HIDS) have lately gathered interest amongst researchers. HIDS is able to detect malicious events on the host system. This article contains a review of different types of IDS and discusses a threat aware of Host-based IDS architecture. Different traditional IDS architectures have been reviewed, and HIDS architecture has been proposed in this article. Dispatcher is a component that distributes the input traffic to different analyzers. This affects the time of detection and accuracy. Equalizer helps in data normalization. The correlation engine reduces the number of alerts that need to be monitored when an attack occurs. This is done by assimilation of similar events into organized groups.

Jin et al. [17] accumulate the properties of a system that includes the audit logs, events across the network, as well as the order of system calls. Network Intrusion Detection Systems like Snort examines the network traffic by monitoring the data packets, and after that it analyses the traffic to identify if it contains the anomalous codes. With the technological advancement of the internet, network security issues have emerged as important concerns in web applications. Intrusion detection components endeavor to determine illegal and illegitimate activities by inspecting user activities across the network. Optimal Intrusion Detection System should be able to discover the intrusions with a high level of accuracy. Lin et al. [27] define a feature depiction technique which syndicates Cluster Centres and Nearest Neighbours (CANN). The proposed technique transforms the features to a single "distance-based feature," which is further sent to a k-Nearest Neighbor classifier. However, this adds to an initial computational overhead incurred in the reduction of the feature dimensions but gives superior results in detection. Experiments conducted on KDD99 dataset indicate that CANN gives higher accuracy, true positive rate as well as false positive rate than other techniques such as k-NN or SVM classifiers. The proposed work has significant contribution as cluster based approaches save the effort on the nodes as the load is distributed among the nodes in the network. However, CANN is unable to detect user to root (U2R) and Root to Local (R2L) attacks.

Zuech et al. [54] discuss Host-based IDS architecture which is based on the examination of system logs. The proposed architecture comprises of five modules including the one for collection of logs and pre-processing, another module for saving, and updating, a module for performing search and analysis, and alarming module. The four modules collect the logs from the system and turn them into records that contain fields that are extracted from the system logs. These records include "Facility" and "Severity" fields, and a header that contains the "Timestamp" and "Hostname" fields. It also contains "Tag" and "Content" fields. The record thus developed is kept in a MySQL database. Regular expressions are used to extract the relevant records. Further, the records extracted from database are converted to numeric values and sent to a back-propagation Neural Network (BPNN) model for further inspection. After the examination is done, the alarm module intimates the user. Khan [20] introduced Host-based IDS which is an ensemble classifier that uses AdaBoost. They have added a cognitive approach that gives higher weights to the weak classifiers. The researcher briefly discusses Host-based IDSs and Network IDSs, and deliberates their architecture along with the applicability. They have also highlighted the drawbacks like more communication and computation cost of certain techniques. An assessment of the threats confronted by the cloud environments has been done. It also includes different intrusion detection and intrusion prevention mechanisms that address the security issues. Mehnaz and Bertino [32] presented a HIDS called Ghostbuster. The IDS profiles the users based on the patterns of accessing the file-systems and it also detects anomalies. The Linux utility blktrace7 has been used to mine sequences of the events of file access. For each user, a profile is created. The profile contains the file access arranged by sizes, frequencies, and the patterns of files that are accessed. Finite state automaton and outlier analysis has been used to detect anomaly. Performance evaluation is done on actual file accesses of in all 77 users that have accessed 560 files over a period of 8 weeks, out of which 4 weeks have been used for training and remaining 4 weeks for testing. Results indicate low false-positive rate and high detection rate.

Besharati et al. [4] proposed (H-IDS) which protect the virtual machines located in the cloud based network. Logistic regression has been used for extracting the relevant features of the classes. Various attacks have been classified using techniques like neural networks, decision tree classifiers and linear discriminant analysis along with bagging algorithm. The suggested method is experimented on NSL-KDD data set. An accuracy of about 97.51% is achieved to detect attacks. Recently, Ribeiro et al. [34] proposed HIDS for Android enabled Mobile Devices. Various Machine Learning algorithms are used for profiling the malware's behaviour. Both benign as well as malicious profiles have been used for training the proposed model. The advantage of the proposed IDS was that it was autonomous and does not need any linking to a server. It majorly uses benign instances along with some malicious examples.

A host intrusion detection system for industrial embedded devices has been presented by Martinez et al. [30]. The research claims to have considered the system, environmental and device specific properties into consideration. The efficacy of the proposed architecture has been tested by developing a prototype of Host IDS for industrial embedded devices. The system has been implemented in a Programmable Logic Controller (PLC) with a Real-Time Operating System. The evaluation has been done by developing hypotheses and test scenarios. Hypervisor-based intrusion detection system for the cloud environment has been proposed by [1]. The proposed IDS are based on multivariate statistical analysis that monitors the changes in order to detect anomalous behaviors. It monitors the individual behavior and correlated instance behavior to detect intrusion. As a departure from the conventional monolithic network IDS feature model, we leverage the fact that a hypervisor consists of a collection of instances, to introduce an instance-oriented feature model that exploits the individual and correlated behaviors of instances to improve the detection capability.

4.2 Network IDS

This system depends on the target system and the associated network. The examination of Network IDS is based on manual or automatic analysis. The security infr-astructure of the system is significantly used in the NIDS. Furthermore, to regulate the incoming and outgoing threats, anti-threat software is deployed on the servers in Network Intrusion Detection System. It is crucial to provide security across several areas such as government, business and industries, as well as educational institutions.

Peddabachigari et al. [40] proposed a CANN technique in which the distance of data and associated cluster center, and also the distance of the data sample and its nearest neighbor within the cluster are calculated. After this, the newly constructed distance-based feature is further used to classify the data sample on a k-Nearest Neighbour (k-NN) classifier that is used for intrusion detection. Higher accuracy and high efficiency in terms of computation are obtained through the proposed approach. Li et al. [24] proposed a model for analyzing the threat for IoT that is based on Artificial Neural Networks (ANN) to control the threats. Its ability to detect DoS and DDoS attacks has been assessed using multi-level perceptron. This article classifies normal and malicious activities in an Internet of Things Network. The Artificial Neural Network module is tested on an Internet of Things network. The results indicate accuracy of 99.4% and it is able to effectively detect DDoS/DoS attacks. Jin et al. [18] developed a fuzzy association rule-based IDS framework. The system is augmented with a hierarchical and bidirectional fuzzy rule based method. The suggested framework makes use of fuzzy rules which are further used for developing the classifiers and at the same time it generates security alerts. Chandrasekhar and Raghuveer [6] suggested a Least Square Support Vector Machine based IDS (LSSVM-IDS) deployed on the proposed feature selection algorithm. The efficacy of the IDS is evaluated on popular datasets, including KDD Cup 99, NSL-KDD, and Kyoto 2006 + . The experimental results indicate that as the proposed feature selection algorithm gives important features for the Intrusion Detection System, the results are more accurate with lesser computational overhead as compared to the other existing methods. Alhamdoosh and Wang [2] reported a two-class problem, i.e., normal and anomaly. The author pointed out that although many ensemble approaches exist, to discover a suitable ensemble technique for a dataset is time-consuming. An ensemble construction method using PSO generated weight was proposed to create an integrated classifier that has better accuracy. Local unimodal sampling (LUS) has been deployed as a meta-optimizer to detect more relevant parameters for Particle Swarm Optimization. In their study, they have taken five subsets chosen randomly from the KDD99 dataset. Ensemble classifiers have also been developed using diverse methodologies and the weighted majority algorithm (WMA) technique. They used the NSL-KDD data set, and address the binary and multiclass problem using 20% dataset for testing. Pawar and Bichkar [39] developed a hybrid technique that can be used to evaluate the intrusion threshold degree which is based on the transaction data's optimal features of the network extracted from the training data. The results demonstrate that the hybrid approach minimizes the computational and time complexity. Also the model was able to achieve a high accuracy of 99.81% and 98.56% on the binary class and multiclass data sets respectively of NSL-KDD.

Hasani et al. [14] proposed the LGP-BA algorithm for selection of features and the selected features are classified using SVM. Higher accuracy and more efficiency are obtained through the proposed approach. Kim et al. [21] proposed a blend of misuse as well as anomaly detection methods for intrusion detection. Sujitha and Kavitha [47] proposed a layered multi-objective PSO algorithm for selection of features. The proposed system is extremely robust and effective. Meta-heuristics based approaches like PSO are able to give reasonably good results in the given time frame. It is able to handle real-time attacks, also the detection is fast and less time consuming. Mazraeh et al. [31] used techniques like Support Vector Machine, Naïve Bayes, and J48, for selection of the features. Since there are several classification techniques that demonstrate more accurate results, the classification techniques used in the paper have limited contribution to the research in IDS. The efficacy of the proposed approach is reported. [30] developed an anomaly NIDS that uses an amalgam of artificial bee colony and AdaBoost algorithms. The results of the experiments on datasets including NSL-KDD and ISC-XIDS2012 are presented. It utilizes the benefits of both artificial bee colony and Adaboost making the proposed work more effective in intrusion detection.

Kesswani et al.[19] have designed an intrusion detection system for smart homes. The system is capable of detecting intrusion with the help of SmartGuard which uses a cluster-based approach for intrusion detection. While detecting intrusion, energy of the nodes is also taken into consideration. The proposed IDS has significant contribution towards intrusion detection in Smart homes and at the same time the cluster based approach distributes the load of intrusion detection among the nodes. And since the technology is advancing day-by-day, such kind of IDS is the need of the day.

Another cluster based approach for detecting intrusion in Internet of Things has been given by Choudhary et al. [8]. Two different intrusion detection approaches, Key Match Algorithm and Cluster based algorithm have been mentioned in the paper. The true positive rate for the Key Mach Algorithm is between 50 and 80% and that of Cluster based algorithm is 76–96% which proves the efficacy of the cluster based approach. Detecting intrusion in IoT based networks is still a challenge and the proposed work tries to address this.

Song et al.[45] suggested an in-vehicle IDS based on Deep Convolutional Neural Network. The system has been designed to detect network intrusion in the Controller Area Network bus (CAN) of the test vehicle. CAN is the standard that is used for communication in in-vehicle networks. The proposed system detects malicious behavior on the basis of learning. The system has been shown to have high detection rate, low false negative rate and reduced complexity. The datasets used in the experiments have been created by the researchers. The results have also been compared to other machine-learning algorithms. Another CNN based Intrusion detection system for industrial Internet of Things (IIoT) has been proposed by Li et al. [25]. The feature data is divided into four parts based on the correlation between them and further the data is converted into grayscale. The experiments conducted on NSL-KDD dataset show high accuracy and are less complex. The proposed approach has been compared to machine learning and deep learning approaches for binary and multi-class classification. Particle Swarm Optimization (PSO) has also been used for optimizing parameters used to detect intrusion as mentioned by Elmasry et al.[11]. A double PSO algorithm has been used to select feature subset and hyper-parameters to address the problems of redundant and irrelevant features. The optimized parameters have been provided to deep learning methods like Deep Belief Network, Deep Neural Networks, and Long Short term recurrent neural networks. The results of the research indicate an improvement of detection rate by 4–6% and reduction of false alarm rate by 1–5% as compared to data that was not optimized. The proposed work has significant contribution as deep learning based approaches give good results without much training of the network. Also the details are hidden from the user thereby reducing the complexity of the system.

5 Comparison of different types of IDS

Since there are different types of IDS, these IDS have different utilities and applications across diverse domains. Signature based IDS detect malicious activity based on Signatures or patterns stored in the database. Such kinds of IDS suffer from the drawback that they are unable to detect any new malicious activity. On the contrary anomaly based IDS are able to detect any new anomaly or behavior.

If we compare Network based IDS and Host-based IDS, former are deployed on the network and can be easily deployed in an existing network. Disadvantages of NIDS are that they are unable to handle large volumes of traffic. Also, they are unable to recognize encrypted traffic and packets that are fragmented. On the other hand, HIDS monitors the traffic on the host logs. Moreover, HIDS can also access encrypted traffic. The drawbacks of HIDS include that it is heavy on the resources of the host and the host may become vulnerable to direct attacks.

In order to overcome the drawbacks of one kind of IDS, hybrid or ensemble approaches are becoming more and more popular these days.

6 Future trends in IDS

It is evident that the modern day's networks are prone to attacks which need to be prevented using effective IDS. More and more research is required to achieve this goal in the evolving network scenarios. Prevention of Intrusion using Intrusion Prevention Systems (IPS) is one such area in which many researchers are progressing. Some researchers are trying to address specific attacks like DoS, DDoS, honeypot, wormhole, blackhole, Sybil attacks etc., while others are trying to explore intrusion detection and prevention in under-explored areas like cloud, Internet of Things, and edge networks.

7 Conclusion

The main objective of this article is to present a systematic survey of various techniques and systems for intrusion detection in network security. Intrusion Detection Systems can protect from external as well as internal attackers while using various types of network services. The intrusion detection system is an emerging research domain, and it has key criticism for the capacities of retorting to crises, plummeting losses due to network attacks, detecting abnormal behavior, enabling the system to respond to the attacks. The authors have presented the motivation and background details of the intrusion detection techniques in this article. The various pros and cons of different IDS techniques and various characteristics of IDS are discussed. In the survey protocol, a few research queries are explored and responses for each query are also provided. A variety of dataset sources are mentioned in this article. The purpose of this paper is to aid the apprentice researchers in this area with intricacies regarding the IDS.

Funding No funding was received.

Compliance with ethical standards

Conflict of interest The author(s) declare that they have no competing interests.

References

1. Aldribi, A., Traoré, I., Moa, B., & Nwamuo, O. (2020). Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. *Computers & Security, 88,* 101646.
2. Alhamdoosh, M., & Wang, D. (2014). Fast decorrelated neural network ensembles with random weights. *Information Sciences, 264,* 104–117.
3. Alharkan, T., & Martin, P. (2012). IDSaaS: Intrusion detection system as a service in public clouds. In *Proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp. 686–687.
4. Besharati, E., Naderan, M., & Namjoo, E. (2019). LR-HIDS: Logistic regression host-based intrusion detection system for cloud environments. *Journal of Ambient Intelligence and Humanized Computing, 10*(9), 3669–3692.
5. Boer, P. D., & Pels, M. (2005). Host-based intrusion detection systems. Amsterdam University. https://www.delaat.net/rp/2004-2005/p19/report.pdf.
6. Chandrasekhar, A., & Raghuveer, K. (2013). An effective technique for intrusion detection using neuro-fuzzy and radial SVM classifier. *Computer Networks & Communications (NetCom), 131,* 499–507.
7. Chang, H., Feng, J., & Duan, C. (2020). HADIoT: A hierarchical anomaly detection framework for IoT. *IEEE Access, 8,* 154530–154539.
8. Choudhary, S., & Kesswani, N. (2018). Detection and prevention of routing attacks in internet of things. In *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference* On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1537–1540). IEEE.
9. Choudhary, S., & Kesswani, N. (2019). Cluster-based intrusion detection method for internet of things. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1–8). IEEE.
10. Danish, S. M., Nasir, A., Qureshi, H. K., Ashfaq, A. B., Mumtaz, S & Rodriguez, J. (2018). Network intrusion detection system for jamming attack in LoRaWAN join procedure. In *Proceedings of the IEEE International Conference on Communications* (ICC), pp. 1–6.
11. Elmasry, W., Akbulut, A., & Zaim, A. H. (2020). Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic. *Computer Networks, 168,* 107042.
12. Folino, G., & Sabatino, P. (2016). Ensemble based collaborative and distributed intrusion detection systems: A survey. *Journal of Network and Computer Applications, 66,* 1–16.
13. Garfinkel, T., & Rosenblum, M. (2003). A virtual machine introspection based architecture for intrusion detection. In Ndss., pp. 1–16.
14. Hasani, S. R., Othman, Z. A., & Kahaki, S. M. (2014). Hybrid feature selection algorithm for intrusion detection system. *Journal of Computer Science, 10*(6), 1015.
15. Hebbal, Y., Laniepce, S., & Menaud, J. M. (2015) Virtual machine introspection: Techniques and applications. In *Proceedings of the 10th International Conference on Availability, Reliability and Security*, pp. 676–685.
16. Hore, P., Hall, L. O., & Goldgof, D. B. (2007). Single Pass fuzzy C means. In *Proceedings of the IEEE International Fuzzy Systems Conference*, pp. 1–7.
17. Jin, H., Xiang, G., Zou, D., Wu, S., Zhao, F., Li, M., et al. (2013). A VMM-based intrusion prevention system in cloud computing environment. *The Journal of Supercomputing, 66*(3), 1133–1151.
18. Jin, S., Diao, R., & Shen, Q. (2012). Backward fuzzy interpolation and extrapolation with multiple multi-antecedent rules. In *Proceedings of IEEE International Conference on Fuzzy Systems*, pp. 1170–1177.
19. Kesswani, N., & Agarwal, B. (2020). SmartGuard: An IoT-based intrusion detection system for smart homes. *International Journal of Intelligent Information and Database Systems, 13*(1), 61–71.
20. Khan, M. A. (2016). A survey of security issues for cloud computing. *Journal of Network and Computer Applications, 71,* 11–29.
21. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications, 41*(4), 1690–1700.
22. Larson, D. (2016). Distributed denial of service attacks–holding back the flood. *Network Security, 2016*(3), 5–7.
23. Li, T., Li, Q., Zhu, S., & Ogihara, M. (2002). A survey on wavelet applications in data mining. *ACM SIGKDD Explorations Newsletter, 4*(2), 49–68.
24. Li, Z., Sun, W., & Wang, L. (2012). A neural network based distributed intrusion detection system on cloud platform. In *Proceedings of the 2nd International Conference on Cloud Computing and Intelligence Systems*, 1:75–79.
25. Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., et al. (2020). Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Measurement, 154,* 107450.
26. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications, 36,* 16–24.
27. Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems, 78,* 13–21.
28. Lin, Y., Zhang, Y., & Ou, Y. (2010). The design and implementation of host-based intrusion detection system. In *Proceedings of the 3rd International Symposium on Intelligent Information Technology and Security Informatics*, pp. 595–598.
29. Liu, A., Yuan, Y., & Wijesekera, D., Stavrou, A. (2009). SQLProb: A proxy-based architecture towards preventing SQL injection attacks. In *Proceedings of the ACM Symposium on Applied Computing*., 2054–2061.
30. Mazini, M., Shirazi, B., & Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University-Computer and Information Sciences, 31*(4), 541–553.
31. Mazraeh, S., Ghanavati, M., & Neysi, S. H. (2016). Intrusion detection system with decision tree and combine method algorithm. *International Academic Journal of Science and Engineering, 3*(8), 21–31.

32. Mehnaz, S., & Bertino, E. (2017). Ghostbuster: A fine-grained approach for anomaly detection in file system accesses. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, pp. 3–14.
33. Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2018). A detailed investigation and analysis of using machine learning techniques for intrusion detection. *IEEE Communications Surveys & Tutorials, 21*(1), 686–728.
34. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajaranjan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications, 36*(1), 42–57.
35. Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. *IEEE Network: The Magazine of Global Internetworking, 8*(3), 26–41.
36. Nitin, T., Singh, S. R., & Singh, P. G. (2012). Intrusion detection and prevention system (IDPS) technology-network behaviour analysis system (NBAS). *ISCA Journal of Engineering Sciences, 1*(1), 51–56.
37. Omer, K. A. A., & Awn, F. A. (2015). Performance evaluation of intrusion detection systems using ANN. *Egyptian Computer Science Journal, 39*(4), 32–42.
38. Patel, A., Taghavi, M., Bakhtiyari, K., & Junior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications, 36*(1), 25–41.
39. Pawar, S. N., & Bichkar, R. S. (2015). Genetic algorithm with variable length chromosomes for network intrusion detection. *International Journal of Automation and Computing, 12*(3), 337–342.
40. Peddabachigari, S., Abraham, A., Grosan, C., & Thomas, J. (2007). Modeling intrusion detection system using hybrid intelligent systems. *Journal of Network and Computer Applications, 30*(1), 114–132.
41. Sabahi, F., & Movaghar, A. (2008). Intrusion detection: A survey. In *Proceedings of the International Conference on Systems and Networks Communications*, pp. 23–26.
42. Seethalakshmi, D., & Nasira, G. M. (2016). Detecting and preventing intrusion in multi-tier web applications using double guard. In *Proceedings of the 3rd International Conference on Computing for Sustainable Global Development*, (INDIACom). 2016.
43. Shar, L. K., & Tan, H. B. K. (2013). Defeating SQL injection. *Computer, 46*(3), 69–77.
44. Shavlik, J., & Shavlik, M. (2004). Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage. In *Proceedings of the International Conference on Knowledge Discovery and Data Mining*, pp. 276–285.
45. Song, H. M., Woo, J., & Kim, H. K. (2020). In-vehicle network intrusion detection using deep convolutional neural network. *Vehicular Communications, 21,* 100198.
46. Stavroulakis, P., & Stamp, M. (2010). *Handbook of information and communication security* (p. 2010). New York: Springer.
47. Sujitha, B., & Kavitha, V. (2015). Layered approach for intrusion detection using multi-objective particle swarm optimization. *International Journal of Applied Engineering Research, 10*(12), 31999–32014.
48. Tan, P. N., Steinbach, M., & Kumar, V. (2013). Data mining cluster analysis: Basic concepts and algorithms. *Introduction to Data Mining*. https://cse.sc.edu/~rose/587/PDF/chap8_basic_cluster_analysis.pdf
49. Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M., & Fischer, M. (2015). Taxonomy and survey of collaborative intrusion detection. *ACM Computing Surveys, 47*(4), 55.
50. Venkatraman, S., & Alazab, M. (2018). Use of data visualisation for zero-day Malware detection. *Security and Communication Networks, 2018*(12), 1–13.
51. Verma, A., & Ranga, V. (2020). CoSec-RPL: Detection of copycat attacks in RPL based 6LoWPANs using outlier analysis. *Telecommunication Systems: Modelling, Analysis, Design and Management*, 75:43–61.
52. Wu, S. X., & Banzhaf, W. (2010). The use of computational intelligence in intrusion detection systems: A review. *Applied Soft Computing, 10*(1), 1–35.
53. Zhang, Y., Li, P., & Wang, X. (2019). Intrusion detection for IoT based on improved genetic algorithm and deep belief network. *IEEE Access, 7,* 31711–31722.
54. Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big Heterogeneous data: A survey. *Journal of Big Data*, 2, Article number: 3.

Maruthi Rohit Ayyagari received his Master's degree in Business Administration from the University of Dallas, Texas in 2014. He started his career as a researcher in the Deep Learning and Network Systems area. He currently consults independently with various hi-tech organizations helping them scale their business using Machine Learning, Artificial Intelligence and Deep Learning Mechanisms. His research interests include character recognition, computer vision, anomaly detection and deep learning.

Nishtha Kesswani is currently working at the Central University of Rajasthan, India. She has a teaching and research experience of over 18 years at Universities across the globe including California State University, SB, USA and University of Ljubljana, Slovenia, Europe. She has visited more than 15 countries and has delivered invited talks at several Conferences and Workshops. She is the recipient of the 2014 UGC Raman postdoctoral fellowship tenable in the USA and 2018 Young Teacher award, BICON 2013 Best Paper Award and BIKAM 2013 Best Research Paper Award. Her current areas of research include Wireless networks and Internet of Things.

Munish Kumar received his Master's degree in Computer Science & Engineering from Thapar University, Patiala, India in 2008. He received his Ph.D. degree from Thapar University, Patiala, India in 2015. He started his career as an Assistant Professor in computer application at Jaito Centre of Punjabi University, Patiala. Presently, he is working as Assistant Professor in the Department of Computational Sciences, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, India. His research interests include Character Recognition, Computer Vision and Pattern Recognition. He is a Professional Member of ACM and IEEE.

Krishan Kumar is currently Professor in Department of Information Technology, University Institute of Engineering and Technology, Panjab University, Chandigarh. He has done B. Tech. Computer Science & Engineering from National Institute of Technology, Hamirpur in 1995. He completed his Master of Software Systems from Birla Institute of Technology & Sciences, Pilani in 2001. He finished his regular Ph.D. from Indian Institute of Technology, Roorkee in February, 2008. He has more than 22 years of teaching, research and administrative experience. His general research interests are in the areas of Network Security and Computer Networks. Specific research interests include Intrusion Detection, Protection from Internet Attacks, Web performance, Network architecture/protocols, and Network measurement/ modelling. He has published 2 national and 2 International Books in the field of Computer Science & Network security. He has published more than 150 papers in national / International peer reviewed / Indexed / impact factor Journals and IEEE, ACM and Springer proceedings. His publications are well cited by eminent researchers in the field.