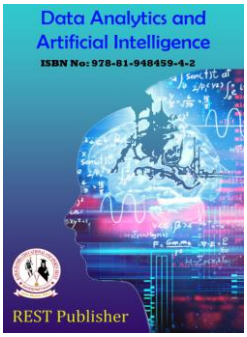
Data Analytics and Artificial Intelligence

Vol: 3(2), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/3/2/24



A Review on Intrusion Detection System and its Techniques

*** A. Kalaivani, R.Pugazendi**

Government Arts College, Autonomous, Salem 7, Tamil Nadu, India.

*Corresponding Author Email: ammu.chin24@gmail.com

Abstract. *Technology development has brought so many threats and hazards at a very high rate in the recent years. The development of application, software tools and its usage in all the fields has brought the awareness about the security. Many mechanisms are used as the security tool such as firewalls, antivirus, spam filters and anti-malware for the security purposes to protect their system and network. Intrusion detection system is a very powerful security system to detect any abnormal or unauthorised access to the system and to the network. This paper is about the study of the importance of intrusion detection, classification of intrusion detection system (IDS), its datasets and usage in various applications. The intrusion detection system has got many developments through its datasets, new technologies and methods but as the technologies increases, the threats of attacking the system and data breaches also increases, so in order to overcome this problem a hybrid framework for the intrusion detection has to be developed to detect the intrusions from the intruder.*

Keywords: *Security, intrusion detection, datasets, classification of IDS, hybrid framework.*

1. INTRODUCTION

Technology has certainly changed how the world works. Modern technology, internet, and IOT undeniably brings a number of advantages across multiple sectors. It also has its share of downsides. The interconnectivity that has tied all devices and systems to the internet has invited malicious forces into the mix, exposing users and business to a wide range of threats. Global attack on IT enabled industries has increased by 28% in the third quarter of 2022 compared to 2021.

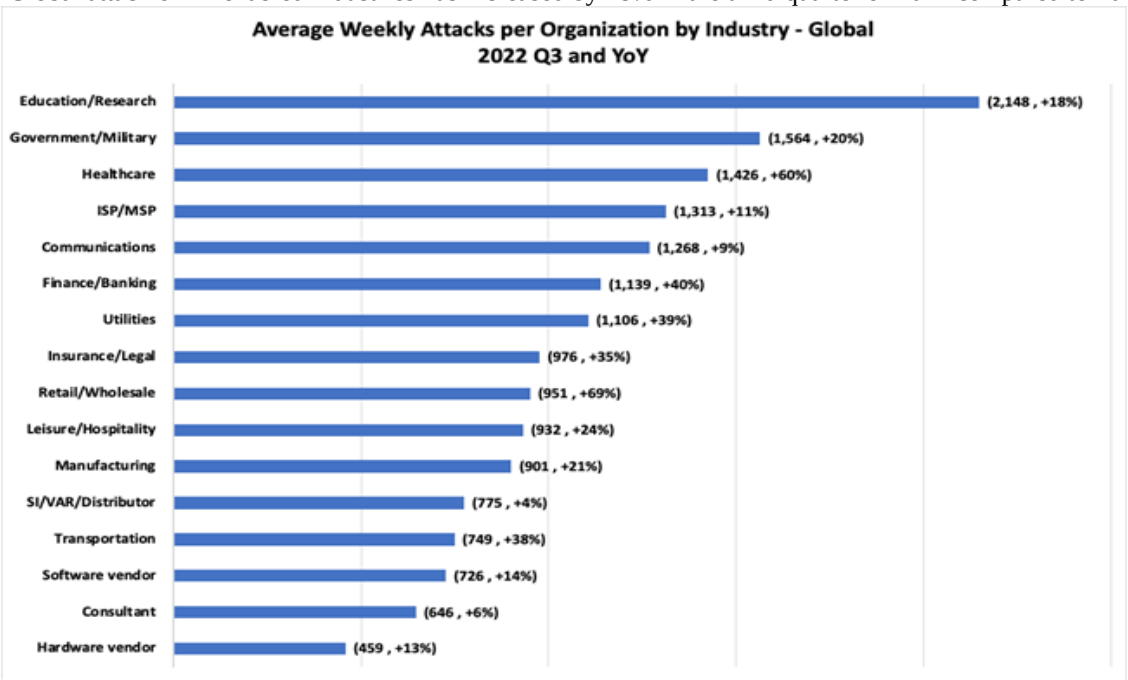


FIGURE 1. Average attack [source: checkpoint]

The figure explains the increase in the attack on the system in all fields. To overcome the intrusion detection system with the hybrid framework has to be developed.

2. INTRUSION DETECTION SYSTEM (IDS)

IDS is a device or software application that monitors a network or system for malicious activity or policy violations. IDS type ranges from single computer to a large network [1] An IDS is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Four main functions performed by IDS are,

- Data collection
- Feature selection
- Analysis
- Action.

Based on the alert given by the IDS, following are the four measuring terms

- TRUE POSITIVE-When an attack is happening, the signal is correctly detected and alerted.
- TRUE NEGATIVE-When no attack is happening, IDS correctly consider the system as normal
- FALSE POSITIVE – When no attack is happening, but still the IDS signals and gives false alert
- FALSE NEGATIVE – When an attack is happening, it is not detected, no signal and no alert is given.

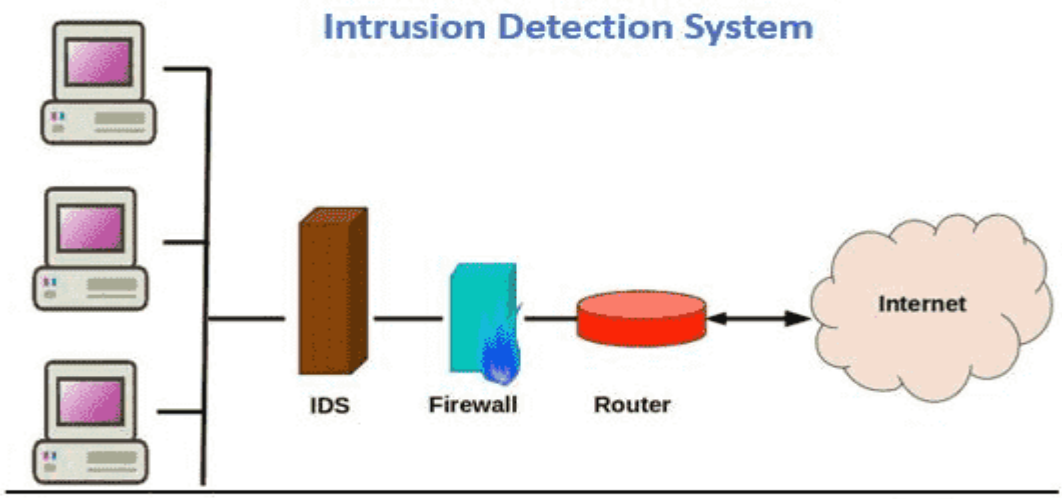


FIGURE 2. IDS on network

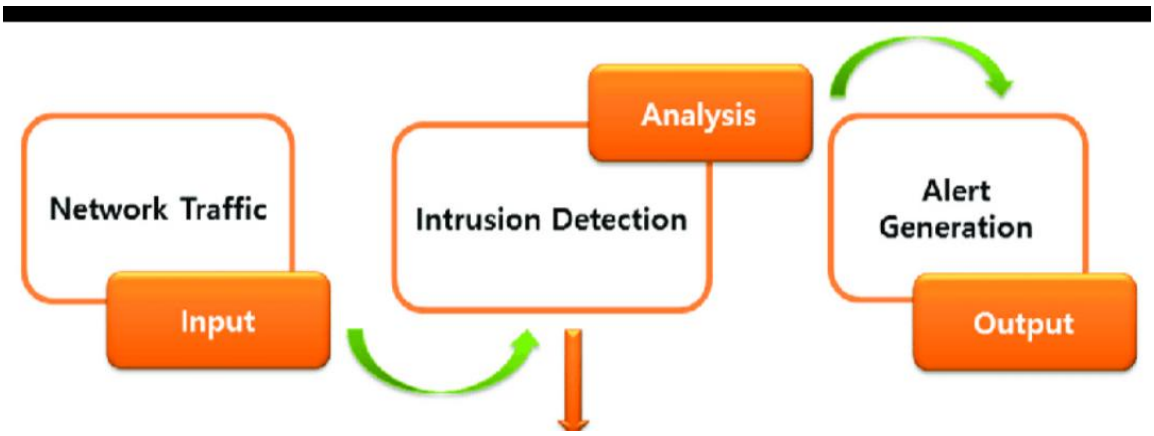


FIGURE 3. Architecture of IDS

The above figure exhibits the position and working of the IDS. The input value is taken from the network traffic then it is analysed in the IDS, if any abnormal behaviour is present then the alert is generated as the output.

3. CLASSIFICATION OF IDS

IDS can be classified based on their, Detection methods, Deployment method, and Response method. Detection Methods: Based on the detection method the IDS can be classified into two important types, Signature based detection method (SIDS): Signature based detection method is a best used for identifying the known threats. It operates by using a pre-programmed list of known threats and their indicators. It detects the intrusion by observing events and identifying patterns that match the signatures which is known as attack. All previous known intrusion is stored in the signature database, when a signature match is found then an alarm signal is triggered. The main idea is to build a database of intrusion signatures and to compare the current set of activities against the existing signatures and raise an alarm if a match is found. Good accuracy is the advantage of this method but zero-day attack is not impossible, as the new signature of the attack when not extracted and stored in the database this is not possible.

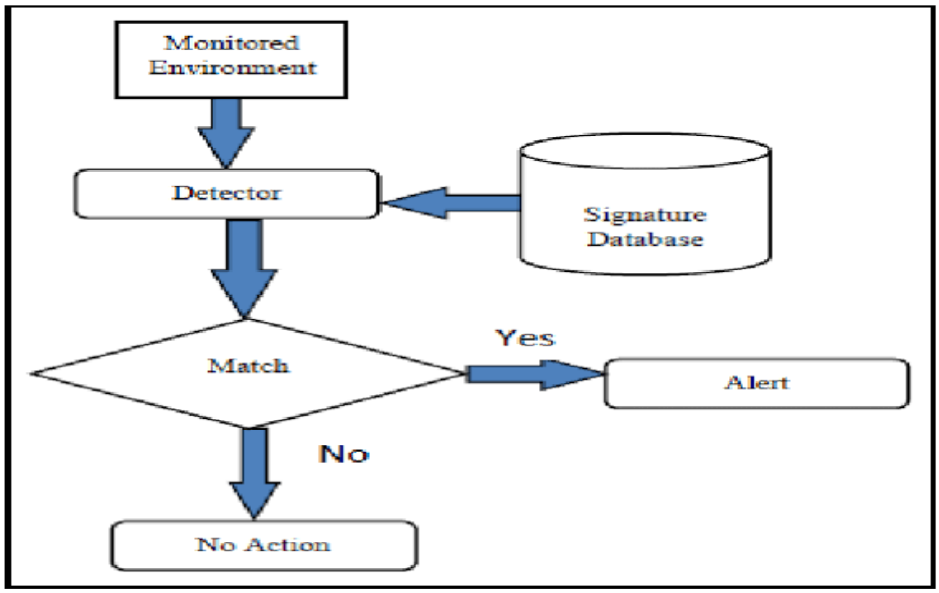


FIGURE 4. Signature based detection method

The figure explains the working of the signature-based system; the threats (attacks) are stored as signature in the signature database. While detecting, if any match signature is detected then alert signal is given else no action will be taken.

Anomaly based detection method (AIDS): The anomaly-based detection is the best used method as it breaks the drawbacks present in the signature-based detection method.

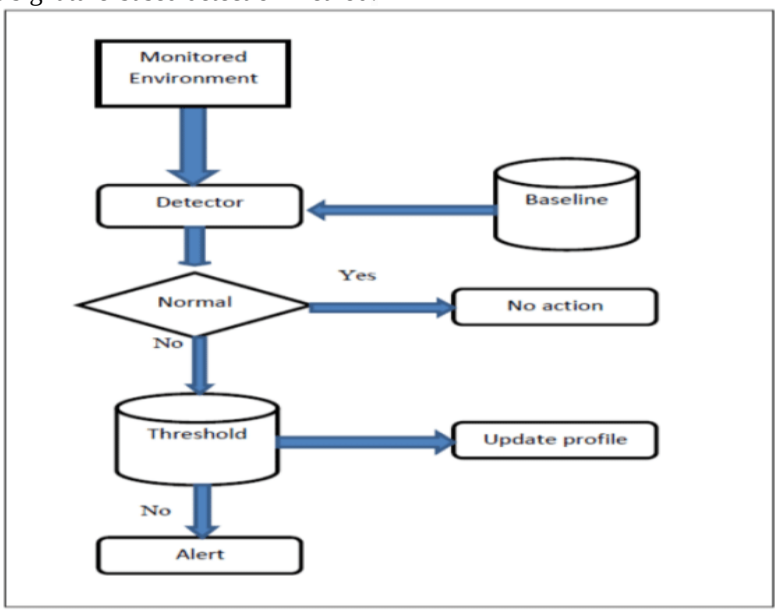


FIGURE 5. Anomaly based detection method.

This method depends on the model which the behaviour of the computer system has developed using machine learning, statistical or knowledge-based methods. Intrusion is detected when a significant deviation is observed between the observed data and model data. Any significant deviation between the observed behaviour and the model is regarded as an anomaly, which can be interpreted as an intrusion.[7]. The assumption for this group of techniques is that malicious behaviour differs from the observed behaviour. Here it comprises of training phase and the testing phase. In the training phase the normal traffic values are used to construct the model for normal behaviour. In the testing phase, the system capacity is improved by introducing the new data (unseen intrusions) to the system [3]. In this way the AIDS has got a good scope, as it has zero-day attack and it is also enhanced using machine learning concepts.

The figure explains the working model of anomaly based detection system, where in the baseline the behaviour of the computer is generated using machine learning, intrusion is detected when there is a deviation from the observed data and the computer model. New threat which is new to the model can be added to it for future detection. The difference between the signature based and anomaly based is given as follows.

TABLE 1. Difference between signature and anomaly

S. No	Topic	Anamoly	Signature
1.	False rate	High false alarm	Low false alarm
2.	Accuracy rate	Low	Medium
3.	Network size	Small	Large
4.	Techniques used	Intelligence based, statistical based	Data mining, Pattern matching
5.	Detection	Both known and unknown attacks	Only well-known attack
6.	Definition	It employs deviation ideas from the standard usage pattern to recognize intrusions	It employs patterns of the well-known attacks to recognize intrusions

Deployment method: Based on the deployment of the IDS, it is further classified into two types. Host based intrusion detection system, Network based intrusion detection system

Host based IDS (HIDS): The first developed type [2] of intrusion detection. The IDS is deployed in one system and the intruder attack is prevented only in that system. HIDS works by analysing and monitoring the internal computing, system level activities of a single system. It works on configuration, system logs, file access, sharing, and modification and application usage.

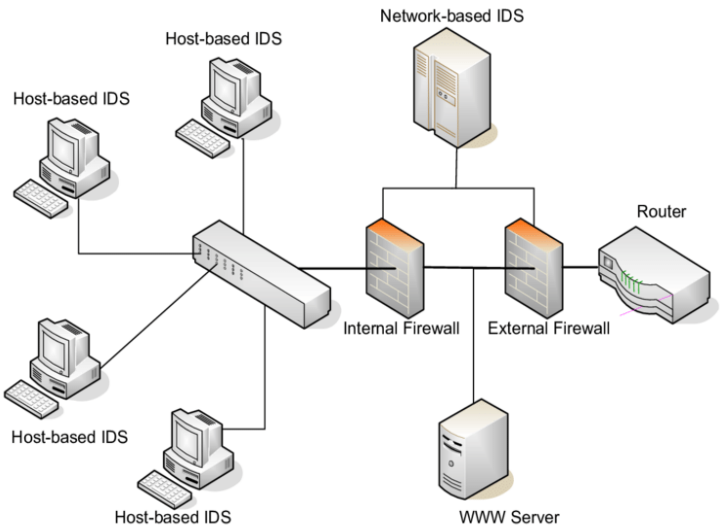


FIGURE 6. HIDS

Network based IDS(NIDS): NIDS is used in an overall network system or on a segment of a network to identify the attacks. Network sensors or applications are the dedicated one which is used for NIDS. It works by analysing and monitoring the activities on the network. NIDS works on the packet level [2]. It checks on the packets, IP address and on the headers part of the packet for any suspicious threat. If found any it is discarded, and the alarm is given.Some of the technologies used by the NIDS to monitor are, Packets headers, Transmissions, Protocols. SNORT is the best example.

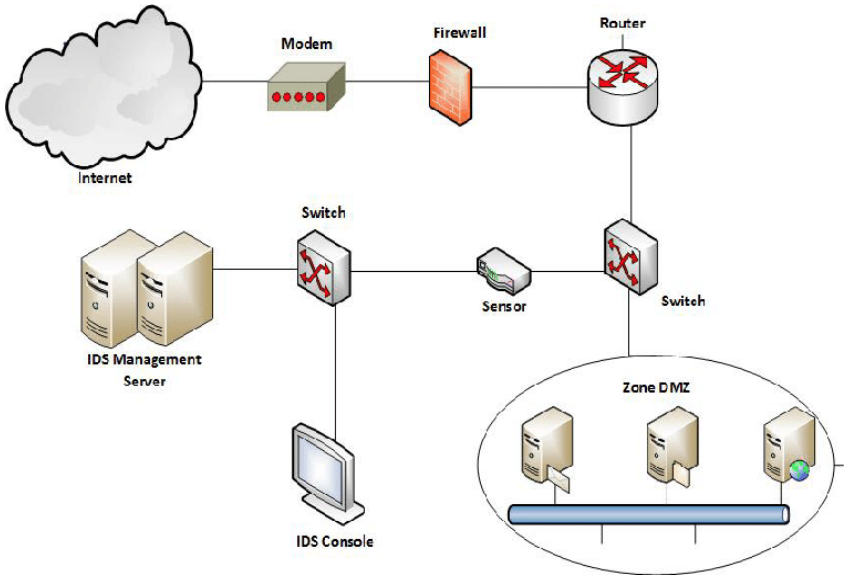


FIGURE 7. NIDS

RESPONSE METHOD: Based on the response method it is further classified into two types. **Passive system:** In this system, the IDS sensor detects [5] a potential security breaches, logs the information about it and signals to the owner.

Active system: In this system, the IPS (intrusion prevention system) auto responds to the malicious activity by reprogramming the firewall to block the traffic from the source

4. TECHNIQUES USED FOR NIDS

The various techniques used for implementing the model for NIDS are as follows,

Statistical -based NIDS: The statistical based intrusion technique depends on the statistical values of the variables used on the network. Statistical metrics such as the median, mean, mode and standard deviation of packets. In other words, rather than inspecting data traffic, each packet is monitored, variables considered for statistical observation [6] are timers, resource overflow flag, log in session. This method uses several models like univariate, multivariate and time series. Univariate is single measure is considered for identifying the abnormal behaviour. Multivariate where multiple measures are included to understand the relationship between multiple variables present in the network. A time series is a series of observations made over a certain time, interval. A new observation is abnormal if its probability of occurring at that time is too low.

Knowledge -based NIDS: Knowledge based technique is the best one to be used for having less false rate, known as expert system method. This method requires creating a knowledge base which reflects the legitimate traffic profile. Actions which are different from this are observed as intrusion. This method is based on human knowledge, in terms of a set of rules that try to define normal system activity [7]. Advantage is it reduces false positive rate, as all the behaviour of the system is known. Only drawback here is having updated knowledge about the network data. This includes the database of the signatures known to be associated with malicious activity.

Machine based NIDS: Machine based NIDS is used in the high dimensional network. Machine learning techniques have been applied extensively in the area of AIDS. Several algorithms and techniques such as clustering, neural networks, association rules, decision trees, genetic algorithms, and nearest neighbour methods, have been applied for discovering the knowledge from intrusion detection the models here are trained with the data and tested for the same. Mathematical models are used to extract information from the large datasets. Few algorithms used here are K-Near, decision tree and K-mean.

5. DATASETS

Datasets are the collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computerise dataset, a systematic manner, which will contain detailed descriptions of intrusions and abstract distribution models for applications, protocols, or lower-level network entities. These profiles can be used by agents or human operators to generate events on the network. The evaluation of Datasets is very important for any IDS approach. The datasets used in the network packets are not available due to the privacy issues [7]. Few available datasets are as follows

- DARPA Dataset: The first dataset, which was collected by connected all computer to an internet and the data was collected from the packets and the flow of information from the source and to target IP address, TCP sessions, log files .This method led to the base for the KDD Cup99 dataset.
- CAIDA: This dataset was collected from the traces of traffic from the Distributed Denial-of-Service (DDoS). When the traffic was interrupted it was analysed and data was collected. The disadvantage of this was it was not able to identify the normal and abnormal traffic due to the diversity in the network.
- CICIDS 2017: This dataset collects the data from the timestamp of the source and destination port, IP address, and the full topology of the network is used with all features and data flow. This dataset includes all types of attacks like denial of service, bot net and web attack.

6. FINDINGS

IDS has becomean important part of all the information system. IDS has to be different when used in different applications. The basic environment of the system has to be studied well, analyse the critical risk involved when implementing, then the dataset has to be built up for the particular field of application. Without the use of IDS system, the threats and attacks to the system and network are more. A more detailed analysis of the network with different operating system, different topology has tobe tested and trained. The IDS which are used currently has few drawbacks in supporting large volume of data, can't detect updated threats and more research on the datasets are required.

7. CONCLUSION

This article provides an overall review of the IDS system and its types, techniques. The detection methods available for the IDS are signature based and anomaly based. Both these detection methods have their own merits and demerits. A hybrid approach of both these methods should be used in the network. A novel model which implements the hybrid collection of different detection methods and techniques has to be developed. The main idea to enhance the IDS is to have the method which handles large volume of data which is not supported by any of the methods which is a capable for the evasion technique should be considered, which a big challenge is. Finally, a hybrid framework which incorporates many methods, different algorithms at different stage of detection in the same network and datasets with different techniques like deep learning should be taken into consideration for research for a strong IDS system.

REFERENCES

[1]. Survey on Intrusion detection system types. By Saud Mohammed Othman, NabeelT.Alsohyle, Fadl Mutaher Ba-Alwi,Amar Thabit zahary,International journal of cybersecurity and digital forensics ,ISSN:2305-001
[2]. A proposed architecture of intrusion detection systems for internet banking,
[3]. Pritika Mehra, International journal of advance foundation and research in science and engineering, ICCICT 2015
[4]. Survey of intrusion detection systems: techniques, datasets and challenges, Ansam Khraisat, Iqbal Gondal, Peter Vamplew & Joarder Kamruzzaman ,Springer Open access, 2019.
[5]. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, Ansam kharisat,Amar Alazah. Springer author open access 2021
[6]. Research on intrusion detection and response, Peyman kabiri, Ali A.Ghorbani
[7]. Research trends in network-based intrusion detection system: A review,
[8]. Satish Kumar, Sunanda Gupta, Sakshi Arora, IEEE access, November 2022