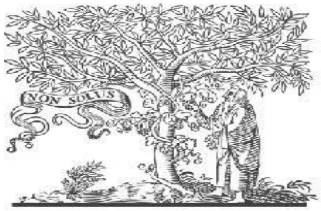
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 22 jul 2020. Link :http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=Issue 07

10.48047/IJIEMR/V09/ISSUE 07/42

Title **Traditional and Machine Learning Intrusion Detection System Approaches: A Comparative Analysis**

Volume 09, ISSUE 07, Pages: 344-362

Paper Authors **Anupoju Venkata Malleswara Rao, Shaheda Akthar**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Traditional and Machine Learning Intrusion Detection System Approaches: A Comparative Analysis

Anupoju Venkata Malleswara Rao[1] and Shaheda Akthar[2]

[1]Research Scholar, Dept. of CSE, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. E-Mail: anupoju.mallesh@gmail.com

[2]Lecturer in Computer Science, Department of Computer Science, Govt. College for Women, Guntur, Andhra Pradesh, India.

Abstract:
Computer and networking technologies play a significant role in our lives nowadays. Many of us rely on these technologies in our day-to-day activities, which include personal work, office work, organization, community work, education, transportation, and communications. Today, most of them discussions on network security tools or techniques used in protecting and defending networks. The traditional methods like firewall, URL filters, mainly focused on the filtering of data and may not sufficient to find all type of attacks always. Among numerous solutions, Intrusion detection systems (IDS) plays a major role in system security and also optimal system for detecting different kind of attacks. In order to stop hackers from harming computer systems, an ideal intrusion detection system can identify intrusions in real time. Different intrusion detection methods, each having advantages and disadvantages, can be used to construct intrusion detection systems. The IDS is being implemented using latest technologies such as Machine Learning Algorithms to classify the attacks and detecting them whenever an attack happens and also to find which machine learning algorithm is best suitable for identifying the attack. The paper presents an overview of the IDS and IPS, differences between IDS and IPS, classifications, methods and various aspects of traditional IDS and also discussed on Machine Learning based IDS, datasets for developing efficient and effective ML based IDS.

KEYWORDS: Cyber Attacks, Network Security, Intrusion Detection System, Intrusion Prevention System, Machine Learning.

1. INTRODUCTION:

The internet is a part of our lives in this digital age, bringing the world closer to us. With the advent of the internet, the possibility of intrusion has become all too ubiquitous. In this virtual environment, there is no escape from attackers and hackers. Internet security has become an issue for enterprises in today's world, and they may be subject to cyber-attacks. As hackers become more sophisticated, identifying breaches becomes more difficult. If the incursions continue, security services such as data confidentiality, integrity, and availability may suffer a loss of trust. Furthermore, there have been increased security threats such as zero-day attacks on internet users. As a result, as information technology has invaded our daily lives, computer security has become critical. It is critical that a system's security controls are configured to prevent unauthorized access to its data and resources.

The process of monitoring a computer system or network's activity and analyzing it for indications of possible incidents—breaches or immediate threats of violations of computer security regulations, acceptable use policies, or standard security practices - is known as intrusion detection. Malware (such as worms and spyware), attackers accessing systems via the Internet without authorization, and authorized individuals abusing their privileges

or attempting to obtain more privileges for which they are not authorized are only a few of the reasons of incidents. Despite the fact that many events are malicious, many others aren't; for instance, someone might incorrectly insert the wrong computer's address and try to connect to another system without authorization [1].

1.1. INTRUSION DETECTION SYSTEM (IDS):

Intrusion detection system (IDS) is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies [2]. A network's intrusion threats, attacks, and malicious activity are primarily identified by intrusion detection systems (IDS), which then produce alerts. The drawback of IDS is that it can only monitor network traffic, much as packet sniffing, and cannot defend against network attacks. IDS essentially analyzes copied packets on a network segment to look for attacks or attacks that have already taken place [3].

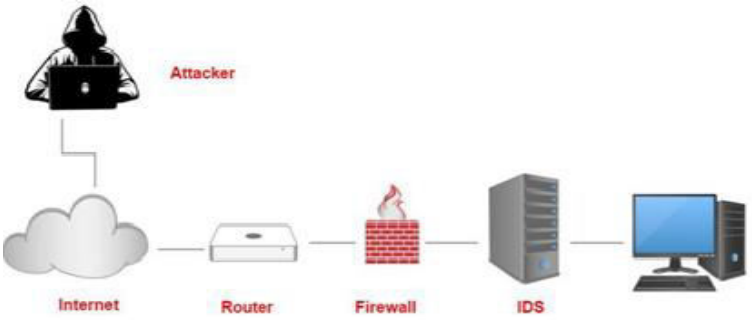


Fig. Intrusion Detection System (IDS)

An IDS is software or hardware that looks for harmful or unauthorized activity on a different host or within a computer network.

The function of an IDS is to identify efforts by cybercriminals to compromise the infrastructure and to produce security alerts (it lacks reaction features like stopping undesirable activity), which it then sends to a Security Information and Event Management (SIEM) system for additional processing.

In contrast to traditional firewalls, intrusion detection systems rely on a set of static rules to restrict traffic between devices or network segments without issuing notifications. The intrusion prevention system (IPS) is an evolution of the IDS concept that not only logs but also blocks threats [5].

I. How Do Intrusion Detection System Works? [6]:

- A computer network's traffic is monitored by an IDS (Intrusion Detection System) to look for any strange activity.
- It examines network data in order to seek for patterns and signs of anomalous behavior.
- To find any behavior that might be an attack or intrusion, the IDS compares the network activity to a set of predetermined rules and patterns.
- The system administrator receives a notification if the IDS finds something that corresponds to one of these rules or patterns.
- After looking into the alert, the system administrator can take appropriate measures to stop any harm or additional infiltration.

II. Advantages of Intrusion Detection System (IDS) [7]:

- An intrusion detection system offers numerous advantages to an organization.
- It monitors all incoming and outgoing network traffic. It detects any evidence of system intrusion. Its primary duty is to deliver an alarm as soon as it detects any activity in the system.
- Its primary duty is to deliver an alarm as soon as it detects any activity in the system. It detects a variety of security incidents. It also aids in determining the number and nature of such suspicious attacks. It also discovers faults and problems with network device setups. This knowledge can be used by an organization to solve the problem. They may modify their security system or use appropriate safeguards.
- Hosts and other network devices are recognized by IDS sensors. They frequently investigate the operating system and network data. The IT team will have less time to do this. As a result, the organization becomes more effective. This will assist the company in reducing staff costs.
- IDS is a tool that can be utilized to fulfill criteria. They provide openness throughout your network. As a result, it aids the firm in complying with various security standards.

III. Challenges of Intrusion Detection System [7]:

There are four key challenges that businesses face when managing IDS systems:

- **Ensuring Effective Deployment:** Organizations must ensure that their wireless intrusion detection system is correctly built and installed to achieve maximum visibility. While deploying IDS can **be challenging, if done incorrectly, it can result in vulnerabilities in critical assets.**
- **Understanding and Investigating Alerts:** IDS warnings provide relatively little information, making it difficult to examine. You may be unaware of what prompted the attack or what extra measures are required to counter a threat. Investigating IDS warnings can also be time consuming and resource intensive, as further information may be necessary to establish the severity of the attack.
- **Managing a High Volume of Alerts:** Because intrusion detection generates the vast majority of attacks, it may create an additional burden on internal teams to identify each one. These system alerts are frequently false positives that are difficult to screen. Furthermore, some intrusion detection systems (IDS) come pre-loaded with an insufficient set of alarm signatures for many organizations.
- **Knowing How to Tackle Threats:** A typical issue that organizations face is a lack of appropriate incident response capability. Identifying a problem is only half the battle; the hardest and critical part is knowing how to respond successfully. For an effective incident response, an expert who understands how to remediate threats and what methods are required to tackle the issue is essential. A home intrusion detection system may cause false alarms on occasion, so keep an eye on the types of threats and how to manage them. The cyber security workforce must be kept up to date on the newest

innovations and changes in IDS and crucial cyber security sectors.

1.2. Intrusion Prevention System (IPS):

Intrusion Prevention System (IPS) is the process of both detecting intrusion activities or threats and managing responsive actions on those detected intrusions and threats throughout the network. IPS monitors real-time packet traffic for malicious actions or that matches certain profiles, triggering the generation of alerts and the ability to discard or block such traffic as it passes through the network. The primary goal of IPS countermeasures is to thwart an ongoing attack [3]. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents [2]. If abnormal traffic passes across the network, IDS will generate a false positive, which implies that it only detects malicious traffic, takes no action, and just provides warnings, whereas IPS detects malicious traffic or suspicious activity and takes measures such as terminating, blocking, or dropping connections.

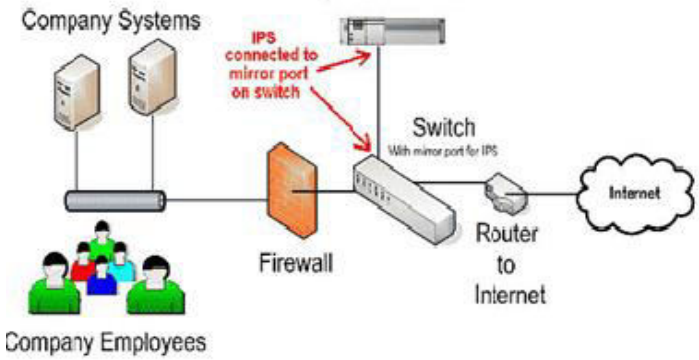


Fig. Intrusion Prevention System (IPS)

1.3. Differences between IDS and IPS Systems:

IDS and IPS were originally designed to overcome deficiencies in most firewalls. IDS are primarily used to identify threats and intrusions in network segments. However, IPS is focused on identifying those threats or intrusions in order to restrict or terminate their activity [3].

The IDS and IPS are list of similar functions like packet inspection, stateful analysis, TCP segment reassembly, deep packet inspection, protocol validation, and signature matching [3].

In terms of the distinction between IDS and IPS, the best illustration of a security gate is, an IDS acts like a patrol car within the border, monitoring activity and looking for anomalous events. However, an IPS acts as a security guard at the gate, granting and denying access depending on credentials and a predetermined rule set, or policy. Regardless of how strong the gate security is, the patrols continue to operate in a system that provides its own checks [3].

An intrusion detection system (IDS) is software or an appliance that identifies threats, unauthorized or malicious network traffic. IDS uses predefined rule sets to inspect the configuration of endpoints to determine whether they are vulnerable to attack (this is known as host-based IDS), and it can also record network activity and compare it to known attacks or attack patterns (this is known as network-based IDS). The goal of intrusion detection is to provide monitoring, auditing, forensics, and reporting of network malicious activities [3].

- Preventing network attacks
- Identifying the intruders

- Preserving logs in case the incident leads to criminal prosecution

The intrusion prevention system (IPS) can not only detect faulty packets created by malicious software, botnets, viruses, and targeted attacks, but it may also take action to prevent such network activity from creating network harm [3].

The attacker's primary goal is to steal sensitive data or intellectual property, and they are interested in anything they can obtain from customer data such as employee details, bank records, and so on. The IPS is designed to protect assets, resources, data, and networks [3].

- IPS stops the attack itself
- IPS changes the security environment

1.4. IDS / IPS Security:

Along with IPS/IDS, some organizations use firewalls and routers. The main distinction between the two is that the firewall merely examines the IP address and port number. It stops communication by utilizing a port number and an IP address. It detects using signatures; if a packet satisfies the criteria or rules established in signatures, it simply forwards that packet; otherwise, it blocks that packet [4].

The firewall is the first line of defense for our network against attackers. It can only detect a limited number of attacks. So we employ IDS/IPS between the front end and back end firewalls to identify and prevent attacks on internal network traffic. By comparing the traffic to the internally established signatures, an IPS/IDS can be installed between that port and the web server. As a result, IDS/IPS adds an extra layer of security to traffic directed at internet-accessible web servers [4].

2. LITERATURE REVIEW:

Various literary works are presented in this section to illustrate the performance of the Intrusion Detection System. The purpose of intrusion detection is to monitor network assets for unusual behavior and network misuse. In comparison to traditional research, most academics in recent years have used ML-based algorithms to detect cyber attacks. Guide to Intrusion Detection and Prevention Systems (IDPS) by Karen Scarfone, Peter Mell, this publication seeks to assist organizations in understanding intrusion detection system (IDS) and intrusion prevention system (IPS) technologies and in designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention systems (IDPS). The publication also provides an overview of complementary technologies that can detect intrusions, such as security information and event management software and network forensic analysis tools [1]. M.Azhagiri, Dr A.Rajesh, Dr S.Karthik, have discussed an overview of IDPS technologies. It explains the key functions that IDPS technologies perform and the detection methodologies that they use. Next, it highlights the most important characteristics of each of the major classes of IDPS technologies and discusses various types of IDPS security capabilities, technology limitations and challenges [2]. Asmaa Shaker Ashoor and Prof. Sharad Gore, have analysed the differences between Intrusion Detection system and intrusion Prevention System (IDS/IPS) technology in computer networks and also analysed on IDS and IPS systems stability, performance and accuracy wise results are compared [3]. Kanika, tells the IDS/IPS security, its classifications, detection method used and the difference between them and also discussed as the future scope of IDS/IPS is to extend its capabilities for other security purposes [4]. Kaspersky IT encyclopedia, GeeksforGeeks, Rebecca Bace and Peter Mell,

discussed on Intrusion Detection System over view, classification of IDS, how does an IDS work, benefits of IDS, Detection methods of IDS, Functions, advantages and challenges of the Intrusion Detection system in the network security [5,6,7]. Indrajeet Kumar, presents an analysis of the performance of various machine learning algorithms in detecting intrusions using a dataset known as the NSL–KDD. The findings show that the Decision Tree and SVM algorithms perform well while the Naïve Bayes algorithm is the worst performer. These findings support the idea that machine learning could be a valuable tool in improving network security [8]. Syam Akhil Repalle and Venkata Ratnam Kolluru, have gone over an overview of machine learning methods and their application in an intrusion detection system [9]. Cuelogic Insights (2019): It has discovered the various machine learning techniques that can be employed to build robust IDS. Because the last decade has seen rapid advancements in machine learning techniques enabling automation and predictions in scales never imagined before. It wasn't long before machine learning techniques were used in reinforcing network security systems. A lot of research has been devoted to this field, and there is a universal acceptance that static datasets do not capture traffic compositions and interventions [10]. Khraisat et al. Cybersecurity (2019), a thorough examination of intrusion detection system approaches, types, and technologies, as well as their benefits and drawbacks. Several machine learning algorithms for detecting zero-day threats are discussed. This study also looks at four common evasion tactics to see how well they work against the most recent IDSs [12]. MIT Lincoln Labs to provide a comprehensive and realistic IDS benchmarking environment [13]. Creech et al. (2014), proposed a HIDS methodology applying discontinuous system call patterns, with the aim to raise detection rates while decreasing false alarm rates [14]. Alazab A, Hobbs M, Abawajy J, Khraisat A, Alazab M (2014), discussed on risk assessment approach to determine an appropriate response action against each attack event and also demonstrated the IIDPS make the detection and prevention of malware more effective [16]. Duque and M. N. B. Omar, a study using k-means data mining algorithm followed by signature-based approach is proposed in order to lessen the false negative rate; and a system for automatically identifying the number of clusters may be developed [17]. S. Y. Ji, B.-K. Jeong, S. Choi, and D. H. Jeong, this study presents a multi-level network abnormality detection method by utilizing reliable rules to detect abnormal behavior, generating a predictive model to detect the exact attacks (i.e. DoS, R2L, and Probe) using the DWT features, and applying a visualization analytic tool to provide further detailed understanding and analysis for users [18]. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, analyzed the entire KDD dataset. The analysis showed that there are two important issues in the data set which highly affects the performance of evaluated systems, and results in a very poor evaluation of anomaly detection approaches. To solve these issues, proposed a new dataset, NSL-KDD, which consists of selected records of the complete KDD dataset [20]. Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA (2012), discussed on a set of guidelines is delineated as prerequisites for a valid evaluation dataset. Introduction and utilization of profiles that can be combined together to create a diverse set of datasets, each with a unique set of features that cover a portion of the evaluation domain. A systematic approach to traffic generation is specified. A sample dataset adherent to the mentioned guidelines is generated through the utilization of profiles [21]. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, the paper evaluates the performance of a comprehensive set of network traffic features and machine learning algorithms to indicate the best set of features for detecting the certain attack categories [22]. Tavallaee, M.; Bagheri, E.; Lu,W.; Ghorbani, A.A, Provided a solution to

solve the two mentioned issues, resulting in new train and test sets which consist of selected records of the complete KDD data set. The provided dataset does not suffer from any of the mentioned problems. Consequently, evaluation results of different research work will be consistent and comparable [23]. Protic, D, presented a review of three datasets, namely KDD Cup '99, NSL-KDD and Kyoto 2006+ datasets, which are widely used in researching intrusion detection in computer networks. The KDD Cup '99 dataset cannot reflect real traffic data since it was generated by simulation over a virtual computer network [24]. Canadian Institute for Cybersecurity datasets are used around the world by universities, private industry, and independent researchers [25].

3. CLASSIFICATION OF INTRUSION DETECTION SYSTEM [6]:

IDS can be classified with the perspective of its deployment or detection methods. A classification taxonomy is given in Figure.

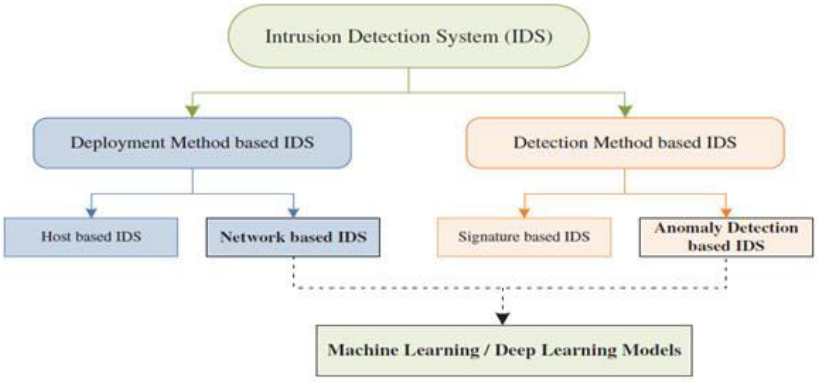


Fig. Intrusion detection system classification taxonomy

IDS are classified into 5 types:

3.1. Network Intrusion Detection System (NIDS): Network intrusion detection systems (NIDS) are placed at strategic points throughout the network to examine traffic from all network devices. It monitors all traffic on the subnet and compares it to a database of known threats. When an attack or unusual behavior is detected, an alarm can be issued to the administrator. Installing an NIDS on the subnet where firewalls are placed to determine if somebody is attempting to penetrate the firewall is an example of an NIDS.

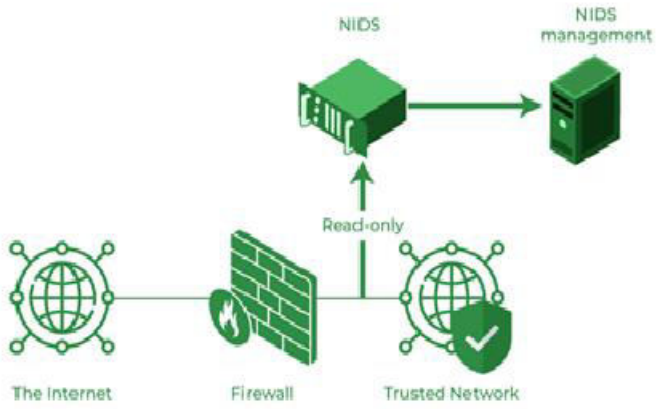


Fig. Network Intrusion Detection System (NIDS)

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

3.2. Host Intrusion Detection System (HIDS): Host intrusion detection systems (HIDS) operate on independent hosts or network devices. A HIDS only monitors the device's incoming and outgoing packets and alerts the administrator if unusual or malicious activity is detected. It compares the current snapshot to the previous snapshot of existing system files. If the analytical system files are modified or destroyed, an alert is sent to the administrator, prompting him or her to investigate. HIDS can be seen in action on mission-critical equipment that are not expected to modify their layout.

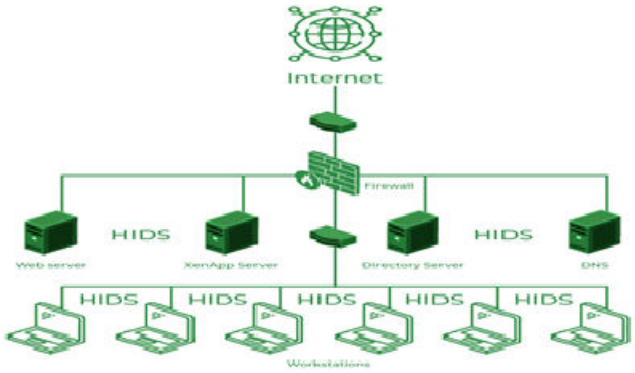


Fig. Host Intrusion Detection System (HIDS)

3.3. Protocol-based Intrusion Detection System (PIDS): A protocol-based intrusion detection system (PIDS) is made up of a system or agent that constantly exists at the front end of a server, regulating and interpreting the protocol between a user/device and the server. It attempts to protect the web server by checking the HTTPS protocol stream on a regular basis and accepting the associated HTTP protocol. Because HTTPS is unencrypted, this system would need to live in this interface before immediately accessing its web presentation layer in order to use HTTPS.

3.4. Application Protocol-based Intrusion Detection System (APIDS): A system or agent known as an application Protocol-based intrusion detection system (APIDS) generally exists within a server cluster. By observing and analyzing communication on application-specific protocols, it detects intrusions. For instance, this would specifically watch the middleware's use of the SQL protocol to communicate with the web server's database.

3.5. Hybrid Intrusion Detection System: A hybrid intrusion detection system is created by combining two or more intrusion detection system methodologies. The host agent or system data is merged with network data in the hybrid intrusion detection system to create a comprehensive picture of the network system. In compared to traditional intrusion detection systems, the hybrid intrusion detection system is more effective. Hybrid IDS is demonstrated by Prelude.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

4. DETECTION METHODS OF IDS [6]:

4.1. Signature-based Method: Signature-based intrusion detection systems detect the attacks based on certain patterns in network traffic, such as the number of bytes, the number of 1s, or the number of 0s. It also detects malware based on the virus's previously known dangerous instruction sequence. Signatures are the patterns recognized by the IDS. Signature-based intrusion detection systems may quickly detect attacks whose pattern (signature) already existing in the system, but it is far more difficult to detect new malware attacks whose pattern (signature) is unknown.

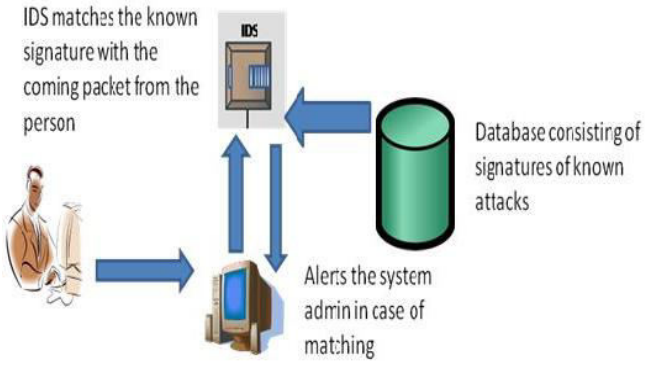


Fig. Signature-based IDS

4.2. Anomaly-based Method: As new malware is generated quickly; anomaly-based IDS was launched to identify unknown malware threats. In anomaly-based IDS, machine learning is used to build a reliable activity model that is compared to anything arriving and is labeled suspicious if it is not found in the model. As these models can be trained based on the applications and hardware configurations, the machine learning-based technique has a better generic property than the signature-based IDS.

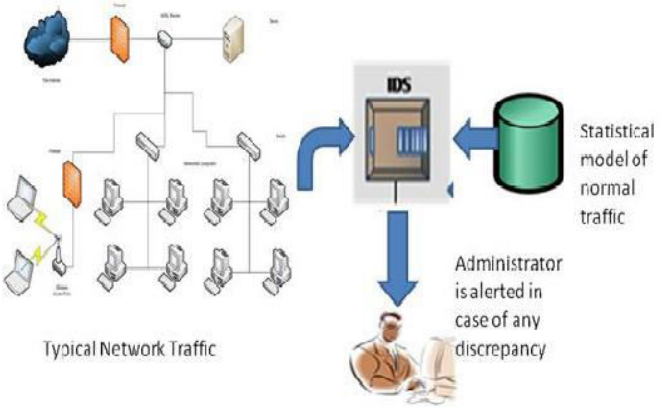


Fig. Anomaly-based IDS

5. DIFFERENCE BETWEEN TRADITIONAL APPROACH VS MACHINE LEARNING BASED APPROACH FOR IDS [8]

- An intrusion detection system (IDS) is an important component of network security since it detects potential threats. Traditional intrusion detection

systems (IDS) describe attack patterns using a set of rules and signatures, which are then used to activate alerts if they match. However, when it comes to detecting unidentified attacks, this approach may be inefficient.

- An intrusion detection system that employs machine learning techniques, on the other hand, may learn and adapt to a variety of attack patterns. The network data can then be examined to determine which patterns are malicious and which are legitimate. This technology is also capable of detecting complex attack strategies that traditional intrusion detection systems are unable of detecting.
- There are significant differences between an IDS that use machine learning techniques and a traditional one.
- **Approach**: The traditional approach of an IDS is to identify possible risks by using a set of predefined rules or signatures. A machine learning-based one, on the other hand, analyzes network traffic using data-driven algorithms to spot patterns that signify malicious or proper behavior.
- **Performance**: Traditional IDS have the major benefit of being able to recognize known threats, but they can also be relatively ineffective in spotting assaults that are unrelated to the signature or rules. An IDS can now recognize sophisticated attack methods that it would not have been able to earlier with the use of machine learning algorithms.
- **Scalability**: The requirement for updates to the signatures or rules in order for them to remain effective restricts the scalability of a traditional IDS. An IDS can learn to recognize new attack patterns and threats by using machine learning techniques.
- **False Positives**: The IDS may produce false positives if its rules or signatures are poorly defined. An IDS can use machine learning to learn about the typical behavior of the network and spot anomalies that would not have been picked up using traditional methods.
- **Training Data**: Traditional intrusion detection systems (IDS) require very minimal training data to function successfully since they rely solely on predetermined rules and signatures. Machine learning-based algorithms, on the other hand, require enormous volumes of training data to find patterns connected to malicious or normal actions.

Although a traditional intrusion detection system (IDS) can effectively identify known threats, but it can also be inefficient when it comes to detecting attacks that do not fit its signatures or regulations. An intrusion detection system (IDS) can learn

to identify patterns associated with malicious or normal behavior using machine learning. Unfortunately, this approach takes a huge quantity of data to train efficiently, and it is vulnerable to attacks.

6. MACHINE LEARNING IN IDS:

A subfield of computer science called "machine learning" is the study of how computers can learn from experience and get better without having explicit programs written for them. The goal of machine learning is to create software that can learn for itself through the use of data. Algorithms that can learn from data and make predictions about it are investigated by machine learning. These formulas are referred to as machine learning formulas. Before using data to create predictions, a machine learning algorithm must first learn. Learning starts with observations or data so that we can seek for patterns in the data and improve our predictions based on the examples given. [9].

After learning from the data, the machine learning algorithm can be used to make predictions on new data. For example, machine learning can be used to monitor the heart rates of hospital patients. The machine learning algorithm is shown the patient's heart rate and the current time during the learning phase. Following learning, the machine learning system can anticipate what the patient's heart rate should be depending on the current time. By comparing the projected and actual heart rates, this can be utilized to determine whether the patient's heart rate is normal [9]. The primary objective is for computers to learn without human intervention and modify their activities accordingly.

6.1. TYPES OF COMPUTER ATTACKS:

Network security analysts can detect intrusion by observing the information obtained from network packets through network flow analysis [11].

- **Denial of Service (DoS):** It is an intrusion attack performed by making the network resources busy and unavailable to the legitimate users.
- **User to Root (U2R):** It is an intrusion attack caused by hampering the authenticity of the user caused by permitting the root access to the intruder.
- **Remote to Local (R2L):** It is an intrusion attack caused by breaking the integrity of the network and permitting the local network access to the intruder.
- **Probe:** It is an intrusion activity performed by scanning the network and gathering all network-related information about the network activities carried out in the network.

6.2. EVALUATING ML FOR AN IDS:

Unsupervised learning algorithms can "learn" the normal network pattern and flag anomalies in the absence of a labelled dataset. It is capable of detecting new sorts of intrusions; however, it is prone to false positive alerts. As a result, just one unsupervised technique, K-means clustering, is covered in this section. To limit false positives, we can use a labelled dataset to train a supervised machine learning model to distinguish between a normal and an attack packet in the network. The supervised model is adept at handling known attacks and can also recognize variations of such attacks. [9, 10].

6.3. USING ML FOR IDS:

Before data can be utilized by a machine learning system, it must first be processed. This implies that features must be picked. Some features can be discovered quickly, while others must be discovered through testing and experimentation. Utilizing every element of a dataset does not ensure the IDS will perform at its peak. The system's processing cost and error rate might both go up as a result. This is due to some functionalities being unnecessary or useless. [9].

7. CLASSIFICATION OF MACHINE LEARNING ALGORITHMS [10]:

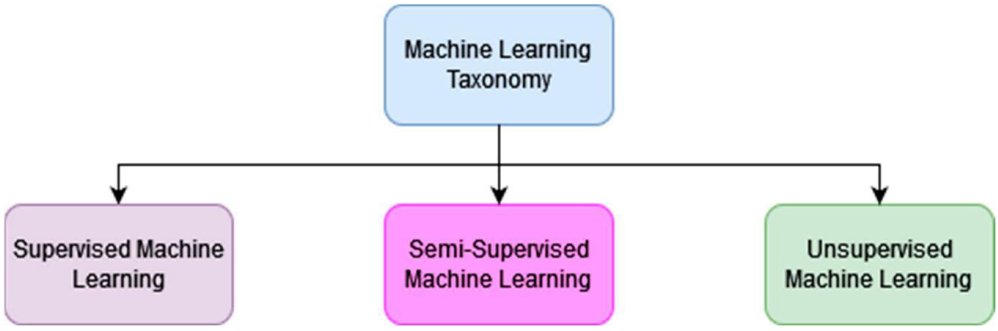


Fig. Main types of machine learning methods

7.1. Supervised machine learning algorithms: may employ what has been learned in the past to predict future events using tagged examples. The method studies a training dataset to provide an inferred function that may be used to predict output values. The system can provide targets for new inputs after adequate training. The computer is given a new collection of examples, so that the supervised learning algorithm may analyze the training data and provide a proper result from labelled data.

7.2. Unsupervised machine learning algorithms: are used when the training data is unmarked or unclassified. Unattended learning investigates how computers might infer a function from unlabeled data

to explain a hidden structure. Without any prior training data, the machine's objective in this case is to categorize unsorted material according to patterns, similarities, and differences. The device is restricted and the structures don't reflect.

7.3. **Semi-supervised machine learning algorithms:** makes use of unlabeled data for training - with a blend of less labelled data and a lot of unlabeled data.

7.4. **Semi-supervised learning falls between unsupervised learning and supervised learning:** When you don't have enough labelled data to construct an accurate model, or you don't have the skills or resources to collect more, semi-supervised techniques can be employed to enhance the quantity of the training data.

8. REVIEW OF INTRUSION DETECTION DATASETS:

An intrusion detection dataset can be created by gathering data from many sources, such as network traffic flows that contain information about the host, user activity, and system parameters. This data is essential to investigate the attack patterns and unusual activities of various network attacks. A router or network switch is used to capture network activity. Network flow analysis is used to evaluate network traffic after collecting incoming and outgoing network traffic. Flow analysis is the process of examining network packet information such as source IP address, destination IP address, source port number, destination port number, and network service type, to mention a few. The network host provides system configurations and user information that the network flow analysis cannot retrieve. For example, information obtained through failed login attempts when monitoring incursion activity [11].

The evaluation datasets are crucial in the validation of any IDS technique since they allow us to examine the proposed method's capability in detecting intrusive behavior. Due to privacy concerns, datasets used for network packet analysis in commercial products are not easily accessible. However, there are a few publicly available datasets that are extensively used as benchmarks, such as DARPA, KDD, NSL-KDD, and ADFA-LD. This section discusses existing datasets used for the development and comparative evaluation of IDS, as well as its features and limitations. [12].

- **DARPA / KDD CUP99:** DARPA (Defense Advanced Research Project Agency) made the first attempt to generate an IDS dataset in 1998, using the KDD98 (Knowledge Discovery and Data Mining (KDD)) dataset. ARPA launched a program at MIT Lincoln Labs in 1998 to create a comprehensive and realistic IDS benchmarking

environment [12, 13]. Although this dataset was a significant contribution to IDS research, its accuracy and ability to address real-world situations were heavily challenged [12, 14]. These datasets were gathered using multiple computers linked to the Internet to simulate a small US Air Force base with restricted personnel. Network packets as well as host log files were gathered. Lincoln Labs created an experimental testbed to collect two months of TCP packet dumps for a LAN, simulating a typical US Air Force LAN. They modeled the LAN as if it were a real Air Force setting, but they mixed in various fake incursions. The collected network packets were around four gigabytes in size and contained approximately 4,900,000 records. The two-week test data contained around 2 million connection records, each of which had 41 attributes and was classified as normal or abnormal. The extracted data consists of a series of TCP sessions that begin and finish at predetermined periods, during which data flows to and from a source IP address to a target IP address, containing a wide range of attacks simulated in a military network environment. The DARPA Dataset from 1998 was used to create the KDD Cup99 dataset, which was utilized in the Third International Knowledge Discovery and Data Mining Tools Competition [12, 15]. These databases are out of date since they do not contain records of recent attacks with malware. For example, attacker behavior varies between network topologies, operating systems, software, and crime toolkits. Nonetheless, KDD99 is still utilized as a standard within the IDS research community and is now being used by researchers [12, 16, 17, 18].

- **CAIDA:** This dataset contains network traffic traces from Distributed Denial-of-Service (DDoS) attacks, and was collected in 2007 [19]. This kind of denial-of-service attack attempts to block normal traffic on a targeted computer or network by flooding the target with a flood of network packets, preventing regular traffic from reaching its legitimate destination machine. One downside of the CAIDA dataset is the lack of variety in the attacks. Furthermore, the acquired data lacks feature from the entire network, making it impossible to discriminate between aberrant and typical traffic flows.

- **NSL-KDD:** This dataset was intended to address the major problem with the KDDcup99 dataset. Tavallaee et al. proposed it in 2009, It retains the

KDDcup99's four attack categories. The NSL-KDD recommends two files, one for training and one for testing. The training set has 126,620 occurrences of 21 different attacks. The testing set contains 22,850 instances of 37 different attacks [13, 20].

- **ISCX 2012:** In this dataset, real network traffic traces were analyzed to identify normal behaviour for computers from real traffic of HTTP, SMTP, SSH, IMAP, POP3, and FTP protocols [13, 22]. This dataset is based on realistic network traffic, which is labeled and contains diverse attacks scenarios.

- **ADFA-LD and ADFA-WD:** Researchers at the Australian Defence Force Academy developed two accessible datasets (ADFA-LD and ADFA-WD) that describe the structure and methods of modern attacks [13, 14]. The datasets contain records from both Linux and Windows operating systems and are derived via the evaluation of system-call-based HIDS. ADFA-LD was built on Ubuntu Linux 11.04 as the host operating system. Because some of the assault instances in ADFA-LD were originated from fresh zero-day malware, this dataset is appropriate for illustrating differences in SIDS and AIDS approaches to intrusion detection. It is divided into three distinct data types, each of which contains raw system call traces. Each training dataset was collected from the host during regular activities, ranging from online browsing to LATEX document production. ADFA-LD additionally includes system call traces from several forms of assaults. The ADFA Windows Dataset (ADFA-WD) is a modern Windows dataset for HIDS evaluation [13, 14].

- **CICIDS 2017:** The CICIDS2017 collection includes information about both benign behavior and novel malware attacks, such as Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet, and DDoS [23]. The timestamp, source and destination IPs, source and destination ports, protocols, and attacks are all labeled in this dataset. This dataset was collected using a complete network topology that included a modem, firewall, switches, routers, and nodes running several operating systems (Microsoft Windows (including Windows 10, Windows 8, Windows 7, and Windows XP), Apple's macOS iOS, and the open source operating system Linux). This dataset includes 80 network flow features extracted from collected network traffic [13, 22].

- **KYOTO 2006**: This dataset was developed by deploying honeypots, dark net sensors, email servers, web crawlers, and other network security measures outside and inside Kyoto University to capture various sorts of traffic. They retrieved 14 statistical features from the 41 features in the KDDcup99 dataset. They additionally extracted 10 additional features to build the dataset, giving each sample 24 features. The most recent Kyoto dataset includes traffic from 2006 to 2015 [23].

- **NSL-KDD:** This dataset was intended to address the primary issue with the KDDcup99 dataset. Tavallaee et al. [12] proposed it in 2009. It retains the KDDcup99's four attack categories. The NSL-KDD recommends two files, one for training and one for testing. The training set has 126,620 occurrences of 21 different attacks. The testing set contains 22,850 instances of 37 different attacks [23].

- **UNSW-NB15:** Australian Center for Cyber Security created this dataset. It was designed to provide traffic that is a mix of everyday activities and attack tactics. Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms are among the nine types of attacks in this dataset. A training set and a testing set are the two files that UNSW suggests. These files include data from the original dataset's various traffic categories, including attacks and regular traffic. There are 2,540,044 records in the original dataset, 175,341 records in the training set, and 82,332 records in the testing set [24].

- **CSE-CIC-IDS2018:** This dataset is the outcome of a collaborative study between the Communications Security Establishment (CSE) and The Canadian Institute for Cybersecurity (CIC), which employs the concept of profiles to develop cybersecurity datasets in a methodical manner. It offers a thorough definition of intrusions as well as abstract distribution models for applications, protocols, and lower-level network components. The dataset contains seven different attack scenarios, including brute-force, heartbleed, botnet, DoS, DDoS, web attacks, and network infiltration from within. The attacker infrastructure consists of 50 machines, while the victim company consists of 5 departments, each with 420 PCs and 30 servers. This dataset contains the network traffic and log files of each victim system, as well as 80 network traffic features derived from collected traffic using CICFlowMeter-V3 [25].

Summary of Datasets in Machine Learning

Dataset Name	Developed By	Features	Attack types	Description
DARPA	MIT Lincoln Laboratory	41	Dos, R2L, U2R, Probe	It does not represent real network traffic, absence of false-positive instances, irregularities in attack data instances.
KDD CUP 99	University of California	41	Dos, R2L, U2R, Probe	It consists of redundant and duplicate data samples.
NSL-KDD	University of California	41	Dos, R2L, U2R, Probe	Refined version of KDD CUP 99 dataset and consist of a limited number of attack types.
DEFCON	Shmoo Group	Flag traces	Telnet Protocol Attacks	Features are captured through the "Capture the Flag" competition.
CAIDA	Center of Applied Internet Data Analysis	20	DDoS	It consists of instances that are very specific to a particular kind of attack or internet activity.
LBNL	Lawrence Berkeley National Laboratory	Internet traces	Malicious traces	It consist of 100 hours of activity specifying the traces of packet header for identifying malicious traffic.
CDX	United States Military Academy	5	Buffer Overflow	This dataset utilized network tools Nikto and Nessus to capture the traffic and was used to evaluate the IDS alert rules.
Kyoto	Kyoto University	24	Normal and Attack sessions	It was developed by deploying honeypots in the network but do not describe any details about the attack types.
Twente	Twente University	IP flows	Malicious traffic, Side-effect traffic, Unknown traffic, and Uncorrelated alerts	The size of the dataset is small and scope of attack types is limited.
ISCX2012	University of New Brunswick	IP flows	DoS, DDoS, Brute-force, Infiltration	This dataset consist of network scenarios with intrusive activities and labeled data instances.
AFDA	University of New South Wales	System call traces	Zero-day attacks, Stealth attack, C100 Webshell attack	This dataset consists of 10 attacks vectors along with the traces of the other data instances but has a limited range of attacks.
CIC-IDS-2017	Canadian Institue of Cyber Security	80	Brute force, Portscan, Botnet, Dos, DDoS, Web, Infiltration	Network profiles are used to generate the dataset in a specific manner.
CSE-CIC-IDS-2018	Canadian Institue of Cyber Security	80	Brute force, Portscan, Botnet, Dos, DDoS, Web, Infiltration	Network profiles are used to generate the dataset in a specific manner.

9. CONCLUSION:

Information security has become a legitimate concern for both organizations and computer users due to the growing confidence with computers and electronic transactions. Different techniques are used to support the security of an organization against threats or attacks. On the other side, attackers are discovering new techniques and ways to break these security policies. Intrusion types of systems are put in place to serve a business needs for meeting an objective of network security. The main aim of Intrusion Detection System is to detect the attacks and malicious activities that occur within a network and to reduce the rate of false positives. By using the machine learning algorithms, the output of the IDS would be accurate, advanced and reliable. The IDS and IPS are to provide a foundation of technology meets to tracking, identifying network attacks to which detect through logs of IDS systems and prevent an action through IPS systems. The study, therefore, recommends the use of Machine Learning approach to implementing an IDS.

This study provided an overview of intrusion detection system methodologies, types, and technologies with their advantages and limitations. This study also provided an overview of the Machine Learning techniques used in implementing IDSs. The results show that the Machine Learning techniques have different strengths and limitations. This paper reviews the datasets and its characteristics of these datasets. In the future, we focus on studying the performance of these datasets with various ML techniques along with incorporating feature engineering and data sampling to address the shortcomings of these datasets. These datasets have been used for performance evaluation of the ML based IDS. The study revealed that there is a need to update the underlying dataset to identify the recent attacks in the field of IDS with improved performance. Traditional IDS (Intrusion Detection System) is a system that detects cyberattacks by using predefined rules or signatures of known attacks. Machine learning IDS is a system that uses machine learning algorithms to learn from data and detect anomalies or patterns that indicate attacks. Machine learning IDS can detect unknown or complex attacks that Traditional IDS may miss, but they may also be vulnerable to adversarial attacks that manipulate the data or the model.

REFERENCES:

[1] Guide to Intrusion Detection and Prevention Systems (IDPS) - Recommendations of the National Institute of Standards and Technology by Karen Scarfone, Peter Mell.

[2] Intrusion Detection and Prevention System: Technologies and Challenges by M. Azhagiri, Dr. A. Rajesh, Dr. S. Karthik.

[3] Asmaa Shaker Ashoor and Prof. Sharad Gore, "Intrusion Detection System (IDS) & Intrusion Prevention System (IPS): Case Study"- International Journal of Scientific & Engineering Research Volume 2, Issue 7, July-2011.

[4] Kanika "Intrusion Detection System and Intrusion Prevention System – A Review Study"- International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013.

[5] Kaspersky IT Encyclopedia, https://www.kaspersky.com

[6] GeeksforGeeks, https://www.geeksforgeeks.org/intrusion-detection-system-ids/

[7] Rebecca Bace and Peter Mell, "Intrusion Detection Systems", Infidel, Inc., Scotts Valley, CA and National Institute of Standards and Technology.

[8] Indrajeet Kumar, "Machine Learning for Network Security: An Analysis of Intrusion Detection Systems" - Turkish Journal of Computer and Mathematics Education, Vol. 10 No.02 (2019), 1075-1080.

[9] Syam Akhil Repalle and Venkata Ratnam Kolluru, "Intrusion Detection System using AI and Machine Learning Algorithm"- International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 12 | Dec-2017.

[10] Evaluation of Machine Learning Algorithms for Intrusion Detection System by Cuelogic www.cuelogic.com/

[11] Ankit Thakkar, Ritika Lohiya, "A Review of the Advancement in Intrusion Detection Datasets"- International Conference on Computational Intelligence and Data Science (ICCIDS 2019).

[12] Ansam Khraisat, Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges"- Khraisat et al. Cybersecurity (2019) – Cyber Security.

[13] MIT Lincoln Laboratory. (1999, June). DARPA Intrusion Detection Data Sets. Available: https://www.ll.mit.edu/ideval/data/

[14] Creech G, HuJ. Generation of a new IDS test data set: Time to retire the KDD collection. In:2013 IEEE Wireless Communications and Networking Conference (WCNC). IEEE; 2013.p.4487–4492.

[15] KDD (1999, June). The 1999 KDD intrusion detection. Available: http://kdd.ics.uci.edu/databases/kddcup99/task.html

[16] Alazab A, Hobbs M, Abawajy J, Khraisat A, Alazab M (2014) Using response action with intelligent intrusion detection and prevention system against web application malware. Information Management & Computer Security 22(5):431–449

[17] S. Duque and M. N. b. Omar, "Using data mining algorithms for developing a model for intrusion detection system (IDS)," Procedia Computer Science, vol. 61, no. Supplement C, pp. 46–51, 2015/01/01/ 2015

[18] S. Y. Ji, B.-K. Jeong, S. Choi, and D. H. Jeong, "A multi-level intrusion detection method for abnormal network behaviors," J Netw Comput Appl, vol. 62, no. Supplement C, pp. 9–17, 2016/02/01/ 2016

[19] P. Hick, E. Aben, K. Claffy, and J. Polterock, "the CAIDA DDoS attack 2007 dataset," ed, 2007

[20] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in 2009 IEEE symposium on computational intelligence for security and defense applications, 2009, pp. 1–6.

[21] Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA (2012) Toward developing a systematic approach to generate benchmark datasets for intrusion detection. computers & security 31(3):357–374.

[22] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in ICISSP, 2018, pp. 108–116.

[23] Tavallaee, M.; Bagheri, E.; Lu,W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp.1–6.

[24] Protic, D. Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ Datasets. Vojnoteh. Glas. 2018, 66, 580–596.

[25] The Canadian Institute for Cybersecurity (CIC) https://www.unb.ca/cic/datasets/ids-2018.html