A brief study on Intrusion Detection System using Machine Learning approach for cyber security.

[1]Pranali R. Landge
Degree College of Physical Education,
HVPM, Amravati,
Maharashtra, India
pranalilandge9@gmail.com

[2]Dr. Swati S. Sherekar
Professor
P.G. Department of Computer Science
Sant Gadge Baba Amravati University,
Amravati Maharashtra, India
swatisherekar@sgbau.ac.in

[3]Dr. Mohammad Atique Mohammad Junaid
Professor & Head
P.G. Department of Computer Science
Sant Gadge Baba Amravati University,
Amravati
Maharashtra, India
mohammadatique@sgbau.ac.in

Abstract
The intrusion detection system (IDS) is the most important tool for identifying malicious activity or cyberattacks. Artificial intelligence is widely regarded as the superior method for developing and adapting intrusion detection systems (IDS) and plays a crucial role in intrusion detection. Intrusion Detection System are part of the defense line of system deployed along with the other security measures, such as access controls, authentication mechanism, and encryption techniques in order to better secure the system against cyber-attacks. IDSs can distinguish between normal and malicious attacks. In this field, intrusion detection systems (IDS) are essential because they keep an eye on system and network activity in order to spot and stop malicious activity.
Keywords: Intrusion Detection System, authentication, encryption

1. Introduction

Intrusion Detection System are becoming more important as cybercriminals continue to develop more new cyber-attacks tools and applications. The way people and organizations function has been completely transformed by the quick development of technology and the widespread use of the internet. This digital transformation, while offering numerous benefits, has also introduced significant security challenges. With the increasing complexity and sophistication of cyber threats, protecting sensitive information and maintaining the integrity of digital systems have become paramount. Intrusion Detection Systems are designed to detect unauthorized access, breaches, and various forms of cyberattacks. Traditional IDS approaches, which rely on static rule-based methods, often fall short in detecting new and sophisticated threats. These limitations highlight the need for more advanced and adaptive solutions that can keep pace with the ever-evolving threat landscape.

2. Background and related work

There is no comprehensive, trustworthy cyber dataset that covers both current and modern-day attacks for network intrusion detection systems, despite the fact that a great deal of research has been done in the fields of artificial intelligence, host-based intrusion detection (HIDS), and network-based intrusion detection (NIDS). Network-based intrusion detection systems (NIDS): Keep an eye on network traffic for questionable activity and examine packets as they move across the network. According to co-authors, the study used an offline method to find shellcode patterns in the data [1]. This section provides important topics that are necessary for understanding the following sections of the paper: intrusion detection system, types, method, component, supervised machine learning and cyber security attacks.

2.1 Types of IDS

IDS can be classified into several types based on their deployment and detection methodologies:

Network-based IDS (NIDS): Monitors network traffic for suspicious activities and analyzes packets traversing the network. NIDS are typically deployed at strategic points within the network to cover all incoming and outgoing traffic.

Host-based IDS (HIDS): Keeps an eye on each host's or device's condition and activity. IDS can detect unauthorized changes to files, system configurations, and logs.

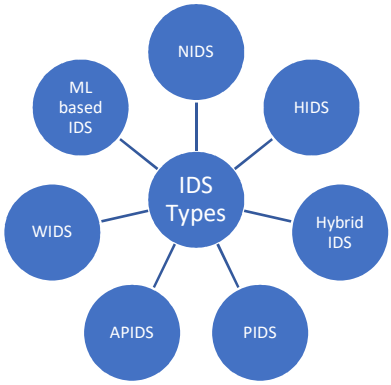

Figure 1: Types of IDS

Protocol-based IDS (PIDS): Protocol-based intrusion detection systems, or PIDS, are frequently installed on web servers to keep an eye on HTTP or HTTPS connections.

Application Protocol-Based IDS (APIDS): Focuses on monitoring and detecting intrusions related to specific application protocols.

Wireless intrusion detection systems (WIDS) are made especially to keep an eye out for threats unique to wireless networks, such as rogue devices or illegal access points. Based on anomalies detects variations from typical network or system behavior.

Machine learning methods, statistical analysis, and pattern matching may be used in this.

2.2 IDS System Methods

IDS employ various techniques to detect intrusions, primarily categorized into following types: Signature-based Detection: This method relies on predefined patterns or signatures of known threats. It is highly effective in identifying known attacks but may struggle with new or evolving threats (zero-day attacks). Signature based detection identifies intrusions by looking for known attack signatures [2].

Anomaly-based Detection: This method establishes a baseline of normal behavior and identifies deviations from the norm. Anomaly-based detection can identify previously unknown threats but may result in higher false positives. Anomaly-based Identifies deviations from normal behavior within a network or system.

Behavior-based IDS: Establishes a system baseline and detects deviations from this baseline to identify anomalies within the system.

2.3 Components of IDS

A typical IDS consists of several key components:
Sensors/Agents**:** Collect data from network traffic or host activities.

Analyzer**:** Processes the collected data to identify potential intrusions. This can involve pattern matching, statistical analysis, and machine learning techniques.

Database**:** Stores information about known threats, patterns, and rules.

User Interface/Alerting System**:** Notifies administrators of potential intrusions through alerts and reports, enabling timely responses.

2.4 Supervised Machine Learning Techniques

Supervised learning and unsupervised learning are two distinct machine learning approaches [3–6] that can be used for automatic intrusion detection. This survey's primary focus is on using supervised machine learning methods for intrusion detection systems. Labeled data is required for supervised learning or classification in order to train a model for detection. The process of classification can be concise in the following steps:

Data collection: the process of gathering information needed to train the classification model. Typically, a feature set that can discriminate between classes is used to characterize the data set. The collection of data is not an easy task, and hence, several benchmark data sets exist such as KDD'99 [7] and NSL-KDD [7], and UNSW-Nb15 [8] and CICIDS2017 [7]. KDD'99 dataset generated using simulation of normal and attacks traffic in a military environment (US AirForce LAN). Rat tcpdump files from nine weeks of simulation are included. 41 features pertaining to intrinsic, content, and traffic are used to characterize the dataset. DoS, Prob, U2R, and R2L attacks are the four types of attacks that are simulated.

NSL-KDD It is a modification to the KDD'99 dataset with solving the problems of redundancy, duplicates, the imbalance of data.

Data reduction: the high dimensionality of the feature space can be problematic and can lead to problems such as the "curse of dimensionality", where there is a relatively low number of training data in a very high dimensional space [9]. That is why data can be transformed into a lower-dimensional space using methods.

Classification: At this stage, Part of the data is used to build the model (training) and another part is used to test the performance of the classification model (testing). A higher number of machine learning algorithms exist in the literature for building the model and will discuss popular types of them, later in this section. The division of data into a training set and testing set only is referred to as a hold-out test. Another common type of test is the N-fold cross-validation test, where the data is divided into N folds, nine of them are used for training and the tenth fold is used for testing the model. Then, another set of nine folds is used for training and the tenth fold is used for testing, and the process repeats. The accuracy is calculated as the average accuracy across all folds[10].

Performance evaluation: the performance of the classification model is evaluated and, usually, the evaluation is done using accuracy and false positive rate (FPR)

2.5 Cyber security attacks

There are two main types of cyber-attacks i.e. active attacks and passive attacks. In the realm of cybersecurity, active attacks are characterized by their direct interference with systems or data, leading to modifications, disruptions, or damage. In contrast, passive attacks concentrate on observing or extracting information without making any alterations to the system. Below is a more comprehensive overview:

Active Attacks:

Definition: Active attacks represent a deliberate effort to breach a system or network, frequently resulting in alterations to data, interruptions in service, or unauthorized access.

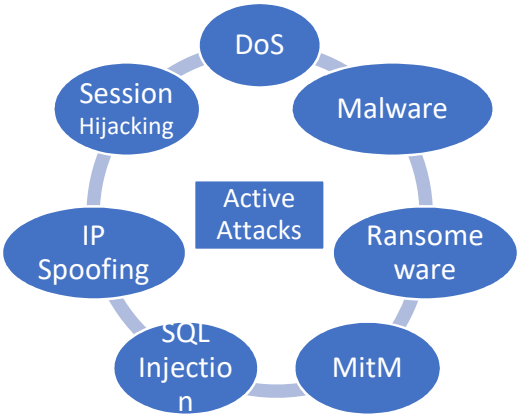

Figure 2: Active attacks

Examples:

- Denial-of-Service (DoS) attacks: Flood a system with excessive traffic, rendering it inaccessible to legitimate users.
- Malware: Introducing harmful software into systems to extract data, disrupt processes, or seize control.
- Ransomware: Encrypting files and demanding a ransom for their decryption.
- Man-in-the-Middle (MitM) attacks: Intercepting communications between two parties to listen in or modify data.
- SQL Injection: Taking advantage of weaknesses in web applications to gain unauthorized access to databases.
- IP Spoofing: Concealing the source IP address to obscure the attacker's identity. Session Hijacking: Seizing control of an active user session.

Detection: Active attacks tend to be more readily identifiable due to their disruptive characteristics and the alterations they impose on systems.

Passive Attack

Definition: In order to obtain information without causing immediate disruption or damage, passive assaults entail monitoring or listening in on network traffic or systems.

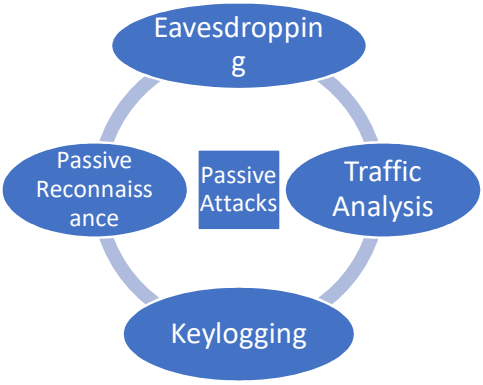

Figure 3: Passive attacks

- Eavesdropping is the practice of intercepting network communication in order to get private data.

- Traffic analysis is the process of examining network traffic patterns in order to spot important information or communication trends.
- Keylogging is the practice of recording keystrokes in order to get passwords or other private data.
- Information gathering about a target system or network without making direct contact with it is known as passive reconnaissance.

Detection: Since passive attacks don't alter or disrupt the system right away, they are frequently more difficult to identify[11].

3 Machine Learning in Intrusion Detection System

By facilitating automated response mechanisms, anomaly detection, and intelligent threat detection, machine learning (ML) has become a potent tool for improving intrusion detection systems. Algorithms that can learn from data, identify patterns, and reach well-informed conclusions without explicit programming are used in machine learning techniques. This feature increases the adaptability of ML-based IDS solutions to emerging and changing threats. Using labeled datasets, supervised learning models like Support Vector Machines (SVMs) and Random Forests can categorize network traffic as benign or malicious, while unsupervised learning models like clustering techniques can use anomaly Detection to find unknown attack patterns [12].

3.1. Methods of Supervised Learning

Labeled datasets are used in supervised learning techniques to teach models to differentiate between benign and malevolent behavior among the crucial methods are:

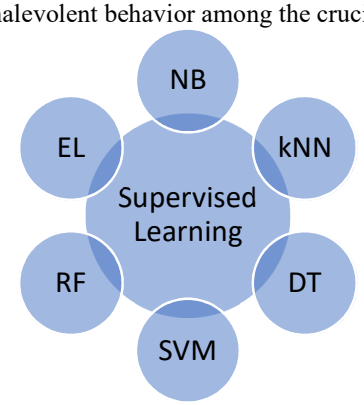

Figure 4: Supervised Learning techniques

1.Naïve Bayes (NB), a probabilistic classifier based on Bayes' theorem, is frequently used for spam detection and Intrusion detection systems.
2. k-Nearest Neighbours (kNN): This distance-based classifier uses feature space's closest data points to determine labels.
3. Decision Tree (DT): An intrusion detection model that uses rules to generate a tree-like structure for decision-making.
4. Support Vector Machine (SVM): An efficient classification algorithm for binary classification tasks in Intrusion Detection systems (IDSs) that uses hyperplanes to separate data.
5. Random Forest (RF): An ensemble of decision trees that decreases overfitting and increases intrusion detection accuracy.
6.Ensemble Learning (EL): A blend of several models (such as boosting or bagging) to improve the detection rate and reduce false positives.

3.2 Methods of Unsupervised Learning

Unsupervised learning techniques identify anomalies or clusters based on patterns and statistical characteristics rather than labeled data important methods consist of

1. K-Means: An algorithm for grouping related data points that can be used to spot unusual network activity.
2. PCA: By simplifying features and spotting departures from typical patterns, Principal Component Analysis (PCA) is a dimensionality reduction technique that aids in anomaly detection.[13]

Conclusion

By facilitating automated threat detection and adaptive responses, machine learning (ML) techniques greatly improve intrusion detection systems (IDS). Although supervised learning models (SVM, RF, and DT) are good at classifying network traffic, they have problems with interpretability and data imbalance. Although unsupervised learning techniques like K-Means and PCA are useful for identifying new threats, they are hindered by their high false positive rates. Future IDS security and dependability may be increased by combining blockchain, federated learning, and explainable AI. To maximize ML-based IDS solutions, research is required to address issues like data imbalance, computational complexity and adversarial attacks. We possibly comprehended that every cybersecurity solution has its pros and cons, and no two businesses will need the same setup. In fact, in most cases, a multilayered approach works best. When you combine more than one type of IDS, you can protect your network from every angle.

References

1. Alex Shenfield, David Day, Aladdin Ayesh, Intelligent intrusion detection system using artificial neural networks, 4 (2) (2018) 95-99
2. V. Kanimozhi, T. Prem Jacob, Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing , ScienceDirect ICT Express 5 (2019) 211–214
3. Bishop, C. M. (2006). Pattern recognition and machine learning. Springer.
4. Witten, I. H., & Frank, E. (2002). Data mining: practical machine learning tools and techniques with Java implementations. Acm Sigmod Record, 31(1), 76-77.
5. https://en.wikipedia.org/wiki/, accessed 1/5/2021
6. Sahasrabuddhe, A., Naikade, S., Ramaswamy, A., Sadliwala, B., & Futane, P. (2017). Survey on intrusion detection system using data mining techniques. Int Res J Eng Technol, 4(5), 1780-4.
7. https://www.unb.ca/cic/datasets/index.html, accessed 1-6-2021
8. www.kaggle.com, accessed 1-6-2021
9. Rust, J. (1997). Using randomization to break the curse of dimensionality. Econometrica: Journal of the Econometric Society, 487-516.
10. Ahmim A, Maglaras L, Ferrag MA, Derdour M, Janicke H. A novel hierarchical intrusion detection system based on decision tree and rules-based models. In: 15th International Conference on Distributed Computing in Sensor Systems (DCOSS). IEEE; 2019. p. 228–33. https://ieeexplore.ieee.org/abstract/document/8804816/
11. Internet Crime Complaint Center. *Internet Crime Report 2021*. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
12. SpringerOpen. *A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges*. https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00077-7
13. Md Boktiar Hossain 1, * and Khandoker Hoque , Machine Learning approaches in IDS, International Journal of Science and Research Archive, 2022, 07(02), 706-715
https://doi.org/10.30574/ijsra.2022.7.2.0303