EXPLORING MACHINE LEARNING METHODS FOR INTRUSION DETECTION SYSTEM: A DEEP DIVE INTO TECHNIQUES, DATASETS, AND PERSISTENT CHALLENGES

SHAIK JOHNY BASHA[1], D. VEERAIAH[2], SUMALATHA LINGAMGUNTA[3]

[1]Research Scholar. Department of CSE, Jawaharlal Nehru Technological University Kakinada, Kakinada, Andhra Pradesh – 533003, India

[2]Professor. Department of CSE, Lakireddy Bali Reddy College of Engineering (A), Mylavaram, NTR District, Andhra Pradesh – 521230, India

[3]Professor. Department of CSE, Jawaharlal Nehru Technological University Kakinada, Kakinada, Andhra Pradesh – 533003, India

E-mail: [1]shaikhjanibasha@gmail.com, [2]veeraiahdvc@gmail.com, [3]lsumalatha@jntucek.ac.in

ABSTRACT

Intrusion Detection Systems (IDS) play a crucial role in safeguarding modern digital infrastructures by identifying potential threats and anomalies in real time. As cyberattacks become more sophisticated, leveraging Machine Learning (ML) techniques in IDS has emerged as a promising approach to enhance detection accuracy, adaptability, and resilience. This paper provides an in-depth exploration of various ML methods applied to IDS, categorizing techniques such as supervised, unsupervised, and reinforcement learning. Additionally, it delves into the most used datasets for training and evaluating IDS models, highlighting their characteristics, advantages, and limitations. Furthermore, the paper addresses the persistent challenges in deploying ML-driven IDS, including issues related to data imbalance, real-time performance, adversarial attacks, and model generalization. Through a comprehensive analysis of current research and future directions, this survey aims to offer insights into the evolving landscape of ML-based IDS, paving the way for more robust and scalable solutions in the face of ever-evolving cyber threats.

Keywords: *IDS Dataset, Cyber security, Machine Learning, Intrusion Detection System (IDS), Network Security*

1. INTRODUCTION

As technology advances, computer networks are becoming increasingly vital in our daily lives. However, this widespread adoption has also made them prime targets for hackers seeking to compromise reliability, availability, and integrity of online data. One of the most significant challenges today is protecting users from unauthorized access and threats on the Internet. IDS are among the key security tools devised to recognize potential intruders within a network or on a host. The growing speed of data transmission and increased internet usage have led to a rise in anomalies, further escalating the frequency of online attacks [1]. As a result, the threat landscape continues to evolve, making cybersecurity an ever more pressing concern. The Skybox Security report on vulnerabilities and threads from 2023 is displayed on Fig. 1. A 23.9% percent increase over the previous year was seen in the graph presented in Fig. 1, which shows that 25096 new vulnerabilities were identified in 2022 [2].

1.1 Intrusion

Intruders are those who engage in activities that aim to bypass the security measures of information systems in a covert manner. This is a series of measures that compromise availability, integrity, and/or confidentiality of data. Preventing unwanted parties from accessing private data is the aim of putting confidentiality safeguards in place [3]. Integrity guarantees that the message remains unaltered throughout the transmission. An unauthorized user alters the content of a communication that a user sends to another user before it reaches the intended recipient. This occurs because of alterations and is known as loss of integrity. According to the availability function, resources must always be accessible to authorized users. Resources become less available because of attacks like interruptions. The types of network assaults are listed in Table 1. The most common ways that intruders cause problems for a system are by breaking in through the operating system of the infected machine, the local network, the Internet, or by taking advantage of a third-party application's vulnerability (middleware). Another common way is by attacking users who try to prevent certain authorized users from earning money, abusing security, or using system privileges [4].

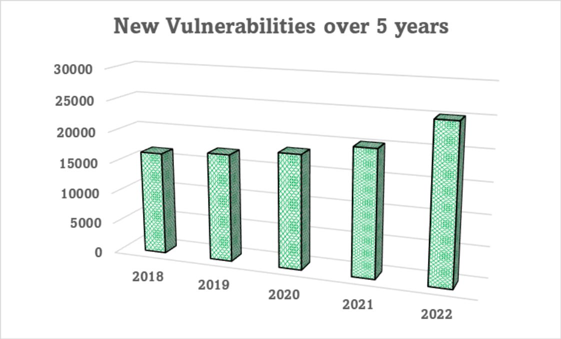

Figure 1: Vulnerabilities over 5 years

1.2 Intrusion Detection

IDS performs forensics after an attack has ended and detects malicious activity in computer systems. Look through network resources for attacks and intrusions that haven't been stopped by precautions (firewall, proxy server, router packet filtering). The goal of intrusion is to undermine a system's availability, confidentiality, or integrity. An approximate comparison between IDS and actual intruder detectors may be made. Fig. 2 accessed from [4] illustrates how abuse-based IDS are used to find breaches of pre-established security guidelines. But things get complicated with the introduction of possible harmful behaviors that cannot be predetermined.

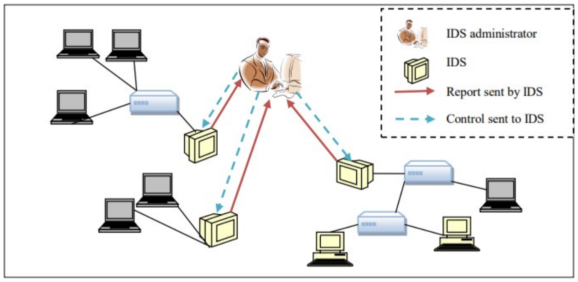

Figure 2: Intrusion Detection System (IDS)

1.3 Classification of Intrusion Detection System

IDSs can be breached by exploiting the location and methodology employed within a given network. By putting IDS module on network, IDSs could be differentiated into 3 classes: network, host, as well as hybrid IDS. The IDS module is mounted on network IDS and can be monitored entirely throughout the network. This IDS investigates malicious activities by examining every packet that passes across the network. In the IDS host, that puts an IDS module on every network client [8]. The module reviewing all incoming and outgoing customer traffic leads to a thorough monitoring of the customer in question. The IDS classification based on various aspects is shown in Fig. 3 accessed from [1].

Two types of IDSs have disadvantages, such as network IDS, which may maximize workload and then neglect any malicious activities, while host IDS may not control all network traffic, and has less workload as compared to network-based IDSs. The Hybrid IDS model is then implemented. In this model, both individual customers and network activities have been tracked at the same time by the IDS modules inside the network and by customers. IDSs can be classified into three different groups depending on detection technique: anomaly, misuse, as well as specification based IDSs. Unsuitable IDS referred to as IDS based on signatures, searches for malicious activities by meeting the identified signatures or attack patterns with the monitored traffic. The traditional IDS don’t detect new types of attacks like ‘Zero-day exploit’. In an AIDS (Anomaly-Based IDS), an attack is observed by profiling normal behavior, and then an alarm is activated if it has deviated. This IDS has the power in the ability to detect unknown attacks. Misuse-based IDS (MIDS) typically perform better than anomaly-based IDS for known attacks. An IDS based on requirements determines a range of rules and restrictions manually to convey normal work. Any deviation from the rules and constraints is flagged as being malicious during implementation.

Statistical Anomaly-based IDS: When abnormal traffic is discovered, an administrator or user is notified by a statistical A-IDS. This type of system monitors standard network activities, such as the type of bandwidth utilized, protocols used, ports used and connected devices (not normal). It is divided once more into a time series, multivariate, and univariate models [2]. By modeling each variable as an independent Gaussian random variable, univariate model parameters define an acceptable range of values for each variable. Two or more variables' correlation is considered by the multivariate model. The temporal sequence model employs an interval timer along with an event counter or resource measure, considering the sequence and spacing between observations as well as their values. An observation is classified as anomalous if its likelihood of appearing at a particular instant is excessively minimal. Various challenges associated with this IDS are:

- Susceptible to an attacker's training
- Unrealistic assumption of quasi-stationary processes
- Setting metrics and criteria might be challenging

Knowledge-based IDS: A knowledge-based IDS (or signature shown in Fig. 4 accessed from [3]) to a database with a previous profile or a previous signature of known vulnerabilities and attacks on the system. The signature here means "documented evidence of intruders" [28, 29]. Hackers always leave their fingerprints on the kind of data packet, how a program is executed, how many tries are made but fail connection issues, and file access. The fingerprints listed above are referred to as signatures. These are employed to recognize and stop similar potential threats in the future. Knowledge-based intrusion detection systems detect infiltration attempts based on these signatures [7]. Various challenges associated with this IDS are:

- Possible to miss a novel or distinct assault
- signature database has to be kept up to date and updated often
- High-quality information and data are difficult and time-consuming to get

Host-based IDS: It is a software (module) installed on a computer system monitored by the network and analyzed on its network interface. A module controls the operating system and keeps data in log files by activating alarms [30, 31]. A HIDS has the sole purpose of monitoring the individual workstations equipped with a module. The entire network cannot be monitored. Alert IDS Protected Computer System Event Generator Analyzer module (decision-making Component) Action module Policies Knowledge-Based Database Policies. Therefore, the HIDS systems shown in Fig. 5 accessed from [5] illustrates how to monitor attack attempts that have occurred on critical servers. Various challenges associated with this IDS are:

- Resource intensity impacting host performance
- Limited Network Scope
- The complexity of managing alerts
- Incomplete network visibility

Anomaly-based IDS: ML along with knowledge-based and statistical approaches, is commonly used to simulate AID [18, 20]. In a network, the model typically represents typical system behavior. Any notable departure from the model in the observed behavior is seen as an incursion. Counts of emails sent, unsuccessful user login attempts, and other features are compared by AIDS. This kind of technology is developed with the idea that malicious activity behaves differently from regular activity. The development of AIDS occurs in two stages: testing and training. AIDSs can identify new types of known attacks in addition to zero-day/novel assaults, which is their primary benefit over SIDS. However, the penalty of this benefit is a higher FAR (“False Alarm Rate”). Recent studies may also make it feasible to determine whether the assailant has AIDS. Within cloud computing, AIDS is capable of identifying unknown abnormalities and assaults at both the network and system levels. It is challenging for AIDS to effectively monitor and identify infiltration since heavy traffic flow happens at multiple levels. A significant false positive rate for AIDS may occur from abnormalities that are mistaken for new normal activity rather than an intrusion or attack.

Network-based IDS: A NIC (“Network Interface Card”) network sensor is usually used in NIDS [44] systems shown in Fig. 6, which regulate incoming as well as outgoing traffic on network and spot abnormal action which might jeopardize security of system [6, 32, 33]. The IDS is positioned along the border of a network segment that monitors all network traffic in that segment. Various challenges associated with this IDS are:

- Increased Network Traffic: recent requests and developments in IT applications have brought network traffic in the middle of hosts to new levels. The NIDS must handle continuous processing and a heavy load
- Reduced Latency: Not only are more and more packages transmitted, but they are exchanged faster.
- It is also a challenge for IDS to gather and process data quickly to avoid delays and storage problems.

Hybrid-Based Approach: Each of the three correlational techniques is attempted to be leveraged by the hybrid-based strategy. A hybrid model that offers warning correlation based on statistical, similarity, and knowledge correlation techniques was presented in the work [29, 30]. Improving alert detection, alert prediction, and assault scenario recognition are their primary objectives. A hybrid intrusion detection system combines >=2 distinct methods for detection. Traditional Hybrid IDS use parallel or sequential detection via AID and SID stacking. Compared to other standalone detection systems like NIDSs and HIDSs, it is more efficient. One of the detection methods from SID and AID is used by NIDSs and HIDSs. As such, the shortcomings of SIDS and AIDS are carried over into NIDS and HIDS. There are three disadvantages to systems that use the SID approach. First off, attackers may easily fool SIDS with malware's polymorphic characteristics, which gives them the opportunity to compromise computer systems. Second, the system becomes inefficient as the size of the signature database increases since it takes longer to evaluate and identify. Finally, and perhaps most crucially, SIDS is not able to identify zero-day attacks as signatures don't match the database of the novel attack type.

By detecting fresh assaults and having a significant generalization power, AIDS solves the problem of SIDS. However, AIDS causes a lot of false alarms because cybersecurity scenarios are changing. ML, knowledge-based methods, and statistical-based methods may all be used to simulate SIDS and AIDS. SID and AID techniques are both used by hybrid IDS to improve attack detection. By employing hybrid intrusion detection systems (IDS), the adverse consequences of standalone SIDS and AIDS can be mitigated. With combination of AIDS and SIDS, hybrid IDS has potential to detect new forms of attacks more accurately and with fewer false positives. SIDS receives the network packets first to identify anomalies. The packets are sent to AIDS for anomaly detection if no intrusion detection is present. When malicious packets are detected, the user is notified, the data is marked as anomalous, and it is stored in the AIDS and SIDS databases. Because there is an increasing danger to cybersecurity and new attacks occur daily, it is imperative to efficiently identify as many threats as possible.

Despite requiring more processing power than standard standalone SIDS and HIDS, HIDS are essential for effective and precise intrusion detection. Given that devices' computing capability is growing with each innovation, robust hybrid IDS shouldn't be dependent on it while developing new devices. However, the expense of owning a strong hybrid IDS-equipped protected equipment goes up. It is necessary to create a potent HIDS that uses less processing resources and provides more effective and precise detection. This may be accomplished by developing a model or classifier by doing a comparative examination of various ML approaches.

Misuse Detection Systems: System keeps track of identified assault patterns and contrasts them with information collected [11]. Every matching model is viewed as an infringement. It cannot identify novel types of assaults since it is a virus detection system. The identification of the misuses depicted in Fig. 7 aims to codify the understanding of assaults and well-defined models and track the presence of these models and models, including the exploitation of digital and sent mail faults utilized on the Internet. On the other hand, It is said that this method compares known attacker actions that attempt system intrusions in the middle of a user's activities. The detection of abuse also uses a knowledge base of information. The knowledge bases on abuse contain specific measures of the different techniques used by hackers to create the knowledge base. Comparison of different IDS like Statistical Anomaly-based IDS, Knowledge-based IDS and Hybrid-Approach on various existing methods was shown in Table 2.

2. ARCHITECTURE OF IDS

The IDS block diagram is shown in Fig. 8. It comprises the subsequent blocks:

- ***Log File:*** Packet sniffer Win Dump collects network packet headers from either the Local Area Network (LAN) or the internet. The Win_Dump data is stored in a file. This file is commonly referred to as a log file.
- ***Data Formatting Unit:*** Several elements in the packet header are used to categorize the data that is gathered and stored in the log file. Certain fields or specified values in these fields are used to identify the protocols used for certain packets.
- ***Log Database:*** It has several tables categorized by various protocols (like ARP, ICMP, UDP, and TCP/IP). There is a single table for every protocol. All the characteristics in each table are specific to that protocol. The database contains formatted data.

- ***Misuse Detection Block:*** Misuse Attacks that are known to exist are found using detection techniques. A lot of cyberattacks use attached signatures. One can use these attack signatures to recognize a specific assault. The collected data packet header is assessed in comparison to predetermined criteria. IDS detects an intrusion and notifies the administrator if the pattern is consistent.

- ***Attack Database:*** The attack database, like the log database, has tables for several protocols. In the attack database are the log database items that have been classified as attacks. Future inferences or table-based analyses of historical system attack statistics may be conducted using this information.

3. INTRUSION DETECTION DATASETS

A significant obstacle facing the scientific community is obtaining appropriate data sets shown in Fig. 9 accessed from [9] to assess different research approaches within the IDS areas. Every day, there are more and more intricate cases of invasions, flaws, security problems, and vulnerabilities. The assessment datasets are vital for the authorization process of any IDS since they enable user to evaluate accuracy of the proposed approach in detecting invasive behavior. Due to privacy concerns, the datasets used in commercial solutions for network packet analysis are not readily accessible. This section discusses characteristics as well as constraints of accessible datasets that are utilized in the construction and comparative assessment of IDS [10].

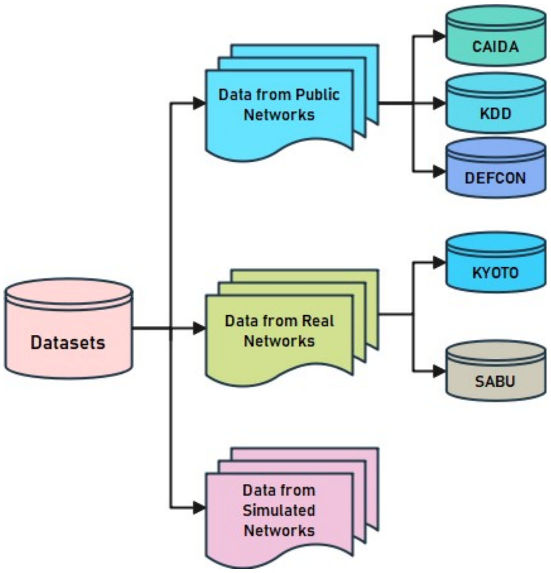

Figure 9: Dataset Sources

3.1 CAIDA

This dataset was gathered in 2007 and includes network traffic traces from DDoS ("Distributed Denial-of-Service") attacks. By bombarding the target with an excessive volume of network packets, this kind of DoS attack aims to stop ordinary traffic from getting to its intended computer and disrupt normal activity on the network. The lack of variation in the assaults inside the CAIDA dataset is one of its drawbacks. Furthermore, it is challenging to discern between aberrant and typical traffic flows since the collected data does not include elements from the whole network.

3.2 KDD CUP 99

It is among the most frequently utilized data sets for ID and is based on DARPA data collection. It is under the category other as it is neither in a conventional packet-based format nor a flow-based format. The data collection lacks IP addresses but does include high-level information like the number of unsuccessful logins attempts in addition to basic information about TCP connections. KDD CUP 99 includes an explicit test subset and covers over 20 distinct attack types (like buffer overflows and DoS attacks). Five million data points are included in the data collection, which is available for free download.

3.3 DEF CON CTF

A well-liked yearly hacker event is called DEF CON. A Capture the Flag (CTF) tournament is part of the event, in which each team must hack the opponent's network while defending their own from the other teams. The competition is usually webcast and accessible in a packet-based format. Owing to the competitive nature of the competition, obtained data consists most of attack traffic, with very little typical user behavior. The website is up to date and gets refreshed every year with fresh information from the CTF contests.

3.4 KYOTO 2006

It is a publicly accessible honeypot data set 22 that comprises just a tiny portion of genuine regular user activity and real network traffic. Kyoto 2006+ is classified as another because packet-based traffic was transformed in a new format known as sessions using the IDS Bro23. Twenty-four features make up each session, fourteen of which provide statistical data obtained from a data set of KDD CUP 99. The next ten parameters are standard flow-based attributes such as time, ports, and anonymized IP addresses. Attacks are indicated using a label attribute. Three years were spent gathering data.

Owing to the atypically extended duration of recording, the data set comprises around 93 million sessions.

3.4 SABU Dataset

This is the first intrusion alert dataset which comprises intrusion warnings gathered from several enterprises' diverse intrusion detection systems. Using eCSIRT.net taxonomy, alerts are categorized and presented in the (IDEA) format. A descriptive data model using a contemporary JSON structure is the IDEA format. Through three organizations and several data sources, about 12 million warnings have been gathered (honeypots, 34 IDS, as well as other data sources). Extensive studies have been conducted on the usage of this dataset for evaluating alert correlation and prediction models.

Multiple datasets have been utilized by certain researchers, such as those shown in Table 3 and Fig. 10, to test their algorithms. With 32.67 percent of the total trials, NSL-KDD is most utilized dataset; KDD Cup 1999 comes in second with 23.76 percent. But DARPA, which accounts for 56.4% of all experiments, is the source of both.

4. TYPES OF ATTACKS

The Intrusion Detection datasets contain different types of attacks. These attacks are classified as:

Denial of Service (DoS): The attackers in this attack have attempted to intercept the original users to obtain any form of service. DoS attacks may be conducted in 2 major methods: by crashing or by flooding systems. Flood assaults occur when the server is overwhelmed with traffic beyond its computational capacity, resulting in server sluggishness and eventual failure. A common type of flood attack comprises:

- *Buffer Overflow Attacks:* The most frequent DoS attack is this one. The objective is to send a network address with a volume of traffic that exceeds the capacity determined by the system's developers. It includes both the attacks listed below and those designed to exploit vulnerabilities specific to certain networks or applications.

- *ICMP Flood:* Devices on this kind of network are misconfigured because fake packets are sent, pinging all of the target computers on the network rather than just one. Then, traffic is intensified by network. Ping of Death or the Smurf attack are additional names of this attack.

- *SYN Flood:* In this kind of attack, the attacker initiates a request to establish a connection with a server, but the handshake is never fully negotiated. This process continues until all available ports are saturated with traffic and no ports are left accessible for connections from authorized users.

Remote to Local (R2L): The attackers' goal is to enter victim's computer without authorization. This happens when a hacker attempts to enter a system across a network without having an account, thus sending packets to that machine to create a vulnerability that would permit the attacker to log on to that machine locally as a user.

User to Root (U2R): To take control of the user's computer, attackers gain local access. Because they enable hackers to run harmful scripts by taking advantage of security flaws, remote-to-local exploits can have disastrous effects on enterprises. Such an attack is employed for eavesdropping, data theft, and business interruption. When it comes to identifying such assaults, manual response methods have a very long dwell detection time.

Probe: Important information about the intended host should be freely obtained by attackers. Most of the assaults fall under the DoS category. Other attack types that can occur in a computer system include DDoS assaults, eavesdropping, spying, and interception.

Eavesdropping: Eavesdropping is listening in on other people's private discussions without their permission.

Snooping: Snooping is a technique for remotely watching over network or computer activities.

Interception: This kind of man-in-the-middle attack modifies communications sent between two devices by intercepting them.

DDoS: malicious effort to obstruct a network's or server's regular flow. Internet traffic is overwhelming the target server and its surroundings. Normal users are thus unable to access the impacted target and its surroundings.

A comparison of accuracy obtained for different datasets on different attacks was shown in Table 4.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. MACHINE LEARNING METHODS FOR IDS

A subfield of Artificial Intelligence (AI) called Machine Learning (ML) obtains knowledge from training data consisting of facts. According to Arthur Samuel (1959), ML is the study of enabling computers to obtain information without the requirement for programming. Prediction is the primary emphasis of ML. Reinforcement, supervised, and unsupervised learning are the 3 main categories that may be used to organize ML approaches [12, 13].

Supervised Learning: It is also identified as classification. In supervised learning data, instances are marked in the training phase. There are several supervised learning algorithms. Bayesian Networks, Gaussian Process Regression, Bayesian Statistics, Artificial Neural Network, Nearest Neighbor algorithm, Lazy learning, Boosting, Hidden Markov Model, Support Vector Machine, K-nearest neighbor, Decision Trees (Random Forrest, CART, ID3, C4.5), Linear Classifiers (Fisher Linear discriminant, Logistic regression, Perceptron, Naive Bayes classifier, SVM), etc. [14, 15, 16, 17, 18, 19].

Unsupervised Learning: Unlabeled data samples are an integral component of unsupervised learning. Clustering is a prominent method employing this learning paradigm. Common unsupervised learners include hierarchical clustering, cluster analysis (specifically fuzzy clustering and K-means clustering), self-organizing map, Eclat algorithm, Apriori algorithm, and Outlier detection (Local outlier factor).

Semi-Supervised Learning: There are 2 forms of learning: semi-supervised and unsupervised. Supervised learning utilizes data of training that is completely labeled and unsupervised learning (without any categorized training data). Studies have demonstrated that classifier performance for IDSs might be improved with less time and money spent when semi-supervised learning is combined with a small quantity of labeled data.

Transfer Learning Approach: Transfer learning is defined as learning that may be applied in other contexts. As such, it is considered a pre-trained model as it is employed to develop model-based tactics.

Instance-Based Learning: "Instance-based learning" is a collection of methods for classification and regression that assesses a query's label or prediction by comparing it to other instances in the training set. Unlike neural networks and decision trees, instance-based learning algorithms are unable to generalize from individual cases.

Reinforcement Learning: Reinforcement learning is the method of a computer interacting with its surroundings to complete a task. An instance from a set of unlabeled examples may be asked to be tagged by a user (such as a domain expert) in a reinforcement strategy.

Deep Learning (DL): Recently, a subset of ML called DL has shown some highly promising results in a variety of applications related to problem-solving. Neural networks with several layers are frequently used in DL techniques. This is done to extract generic characteristics from very large datasets. In several domains, like question answering, natural language processing, sentiment analysis, and language translation, DL algorithms have demonstrated enhanced efficacy.

Single Classifiers: A single classifier or standalone classifier can be created using a single ML method or approach for creating an IDS. This article discusses machine learning methodologies that were frequently employed as standalone classifiers in the analysis of diverse research publications.

Hybrid Classifiers: A hybrid classifier greatly enhances the IDS performance by combining multiple ML methods or methodologies. Employing preprocessing methods based on clustering to remove non-representative training samples from the training set; the clustered samples are then utilized as training samples for pattern recognition to create a classifier.

Ensemble Classifiers: Weak learners are classifiers that outperform a random classifier by a small margin. An ensemble classifier is created when several weak learners are merged with the aim of greatly enhancing the classifier's performance. Some popular techniques for integrating poor learners include majority vote, boosting, and bagging. In some combinations, it has been delivering highly efficient performance, even though it is recognized that drawbacks of individual classifiers aggregate in ensemble classifiers.

A comparison of merits and demerits of various ML methods along with their performance metric was shown in Table 5.

Fig. 11, accessed from [28] exhibits frequency of use of each classifier in literature review. Researchers are using more and more DL methods, like CNN or DNN. It's also evident that a lot of academics use SVM as their classifier owing to its excellent performance in identifying smaller classes. So, they frequently employ a multilayer approach in combining it with other ML techniques. Furthermore, ensemble methods are often employed since they enable combination of various techniques to increase the IDS's efficiency.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. PERFORMANCE METRICS FOR IDS

IDS has several categorization metrics, some of which have several names. As an evaluation tool for an IDS's performance, the following standard performance measures are frequently used to evaluate IDS:

- **TPR (True Positive Rate) (Recall):** It is computed as ratio of total number of attacks to number of successfully predicted assaults. TPR is 1, which is quite uncommon for an IDS if all intrusions are observed. TPR is also referred to as sensitivity or DR. TPR may be statistically symbolized as shown in Eq. 1:

$$TPR = \frac{TP}{TP + FN} \tag{1}$$

- **FPR (False Positive Rate):** It is computed as ratio of total quantity of normal occurrences to number of normal cases which are incorrectly labelled as attacks as shown in Eq. 2:

$$FPR = \frac{FP}{FP + TN} \tag{2}$$

- **False Negative Rate (FNR):** False negatives occur when a detector reports something as normal even when it is incapable of identifying an issue. FNR may be expressed statistically as follows as shown in Eq. 3:

$$FNR = \frac{FN}{FN + TP} \tag{3}$$

- **Precision:** Ratio of accurately anticipated attack samples to all expected attack samples is known as precision shown in Eq. 4.

$$\text{Precision} = \frac{TP}{TP + FP} \tag{4}$$

- **CR (Classification Rate) or Accuracy:** The IDS's ability to identify typical or unusual traffic behavior is evaluated by the CR. It is defined as proportion of all cases that were accurately forecasted in every situation shown in Eq. 5:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{5}$$

- **F-Measure**: This relates to Recall and Precision's harmonic mean. It helps to give a more thorough assessment of the system by displaying differences among 2 metrics and determining if solution is balanced. The F1-Score or F-Score are other names for this metric shown in Eq. 6.

$$F - Measure = 2 \times \frac{(\mathbf{Precision} * \mathbf{Recall})}{(\mathbf{Precision} + \mathbf{Recall})} \tag{6}$$

- **ROC (Receiver Operating Characteristic) Curve:** FPR and TPR are te x- and y-axes of ROC, correspondingly. TPR as a function of FPR at various cut-off points is displayed on a ROC curve. A pair of FPRs and TPRs that satisfy a certain decision criterion is represented by each point on the ROC curve. When categorization criterion is adjusted, a new point on the ROC is selected with a new TPR and FAR. When there is no overlap between the two distributions, a test has perfect discrimination, as indicated by a ROC curve with a pass via top left corner (100% sensitivity, 100% specificity).

Fig. 12 displays the study of the metrics applied to evaluate the many solutions examined. The two most often utilized measures are DR (Recall) and accuracy. Those measurements are the most crucial for determining how well a solution is. As a result, they ought to be applied consistently when assessing an IDS's efficiency. Nevertheless, given that it shows if the system is successful in recognizing attack samples, even from tiny classes, F-measure needs to be applied more frequently when evaluating an IDS.

This study encompassed a collection of scholarly articles published between 2017 and 2023. These articles focused on ways for classifying data and utilizing deep learning methods for intrusion detection systems. These strategies can also be utilized for feature engineering to pick important features that enhance performance of IDS. Numerous IDS datasets have employed these strategies to assess performance. The IDS evaluation utilized standard datasets like NSL-KDD and KDD CUP 99. The precision and rate of identification attained by several machine learning in addition to deep learning techniques, utilizing unique feature selection means, for KDD CUP 99 dataset are presented in Fig. 12, 13 and 14, correspondingly.

7. RESEARCH CHALLENGES

The primary research challenges for IDS are highlighted in this section.

- ***Unavailability of Recent Datasets:*** The study has drawn attention to the lack of up-to-date datasets that depict novel network threats. Most of the methods investigated failed to identify zero-day attacks due to inadequate training of the models with a sufficient variety of attacks. To develop a robust and effective Intrusion Detection System (IDS), it is necessary to train it using an extensive dataset that encompasses the latest assaults. The dataset should include both classic and contemporary attacks to enable the Intrusion Detection System (IDS) to acquire knowledge about the significant characteristics of each attack for the purpose of detection. Thus, a dilemma faced by researchers is the need to obtain a current dataset that encompasses enough samples from various categories of attacks.

- ***Lower Detection Accuracy for Minor Classes:*** The study also shows that most existing solutions are ineffective at recognizing minor classes while having exceptionally high overall accuracy in identifying deviant behavior. The source of this issue is unbalanced datasets. Consequently, minor classes exhibit a reduced level of precision in comparison to major classes.
- ***Low Performance in a Real-World Environment:*** IDS also has difficulties since they don't test in actual scenarios. Most of the solutions under study were evaluated on outdated datasets that did not accurately represent network traffic in the present day. Moreover, no real-world data was used to test any of the solutions. Therefore, it's uncertain which of these strategies will work effectively in a practical setting. Thus, ensuring that future ideas are evaluated in a real-world setting to verify their usefulness will be one of the biggest difficulties moving forward.
- ***Resources Consumed by Complex Models:*** As demonstrated in one of the previous sections, the majority of IDSs are extremely complicated and time- and resource-consuming. The effectiveness of IDS in a real-world setting may be impacted by this need. Using multi-core GPUs is one option to reduce the required amount of time, however, this is a costly solution. To expedite processing, the created algorithms must employ feature extraction to determine which features are most crucial to monitor.
- ***Use of Feature Extraction:*** It's only recently that feature extraction has been used in IDS systems. Still, feature extraction stands out as one of the most effective ways to lower the model's complexity.

8. RESEARCH STATEMENT

Majority of IDS research is done utilizing expert rules and traditional (signature) based methods. These approaches are laborious and inefficient because they require manual procedures, which renders them insufficient [33]. For this reason, ML techniques have been introduced, where the procedures are automated. Researchers have designed comprehensive ML systems for IDS, but most ML algorithms have not found more effective ways to perform a more accurate classification of the datasets. This is because, despite the introduction of ML techniques, most of them are trained on a single, large dataset, making them susceptible to over-fitting when new kinds of attacks are posed. Therefore, one should not overstate the importance of research to identify a model with improved detection accuracy. Furthermore, many studies in this field only utilize one dataset; yet, to evaluate IDS models, a hybridized dataset must be used.

9. COMPARISON WITH PRIOR WORKS AND NOVEL CONTRIBUTIONS

9.1 Previous Research

Many prior studies have focused on applying machine learning (ML) methods to Intrusion Detection Systems (IDS). Key trends include:

- ***Supervised Learning Techniques:*** Earlier works like those using Support Vector Machines (SVM), Decision Trees, and Neural Networks demonstrated high accuracy but struggled with issues like data imbalance and detecting zero-day attacks.
- ***Hybrid Approaches:*** Combining techniques (e.g., anomaly detection with misuse detection) improved accuracy and reduced false positives but required high computational resources.
- ***Dataset Dependency:*** Most studies relied on outdated datasets like KDD CUP 99 and NSL-KDD, which do not capture modern attack patterns effectively.
- ***Deep Learning Advancements:*** Recent research, such as employing Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), improved detection accuracy but introduced challenges in terms of scalability and real-time deployment.

9.2 Differentiation and Novelty of this Work

- ***Comprehensive Evaluation of ML Techniques:*** Unlike most works that focus on a single method or dataset, this paper provides an extensive review of supervised, unsupervised, and reinforcement learning techniques applied to various IDS challenges.
- ***Focus on Persistent Challenges:*** The study addresses critical issues such as data imbalance, real-time performance, and adversarial attacks, which are often overlooked in existing research.
- ***Dataset Analysis:*** The paper highlights the limitations of commonly used datasets and suggests the need for more comprehensive, up-to-date datasets to improve model robustness.
- ***Practical Insights:*** By exploring practical deployment challenges like computational resource requirements and high false alarm rates, the work provides actionable insights for future researchers.

9.3 Justification of Novelty and Importance

- ***Contextual Relevance:*** This work's emphasis on persistent challenges like adversarial attacks and real-time IDS performance fills a gap in the literature, making it highly relevant in today's cybersecurity landscape.
- ***Practical Utility:*** The study not only critiques existing methods but also provides a roadmap for designing more robust and scalable IDS solutions.
- ***Future Directions:*** By highlighting the need for integrating newer datasets and optimizing feature selection, the paper paves the way for innovative research that can address both theoretical and practical challenges in IDS.

10. POTENTIAL APPLICATIONS OF THE WORK

The findings of this study have significant applications in modern cybersecurity frameworks. Specifically, the insights derived from the evaluation of machine learning techniques for Intrusion Detection Systems (IDS) can be utilized in the following applications:

- ***Real-Time Network Security:*** The discussed methodologies can enhance the efficiency and accuracy of real-time IDS in identifying and mitigating cyber threats. By addressing persistent issues such as data imbalance and false positives, these systems can ensure uninterrupted protection of critical infrastructures like banking systems, healthcare networks, and industrial IoT.
- ***Adaptive Threat Management in IoT Networks:*** With the growing adoption of IoT devices, which are particularly vulnerable to cyberattacks, the optimized IDS models suggested in this study can provide lightweight yet robust security solutions. This includes detecting anomalies in low-resource environments where traditional IDS may not perform effectively.
- ***Zero-Day Attack Detection:*** The study's focus on hybrid approaches combining anomaly-based and misuse detection makes it applicable for identifying previously unseen attacks, such as zero-day vulnerabilities, in enterprise and government networks.
- ***Enhanced Security for Smart Grids and Critical Systems:*** Given the increasing complexity of smart grids and critical systems, integrating the reviewed ML-based IDS solutions can safeguard against evolving attack vectors while ensuring operational continuity.
- ***Cloud and Edge Computing Security:*** The study's results can be extended to cloud and edge environments where IDS models can be deployed to monitor and secure data exchanges, offering scalable protection for distributed systems.

11. CONCLUSION

This research sets out to address key questions in Intrusion Detection Systems (IDS) using Machine Learning (ML) techniques, focusing on overcoming challenges such as data imbalance, adversarial attacks, and computational inefficiencies. By categorizing and comparing ML methods (supervised, unsupervised, and hybrid approaches), the study highlights their strengths and limitations, offering a deeper understanding of their applicability to modern cybersecurity threats. A critical gap identified is the reliance on outdated datasets like KDD CUP 99 and NSL-KDD, emphasizing the need for updated, real-world datasets to enhance model training and validation. Persistent challenges, including high false positive rates, scalability constraints, and vulnerability to adversarial attacks, remain areas for future innovation. This study provides insights into the need for IDS solutions that balance detection accuracy, resource efficiency, and adaptability to emerging threats, advocating for interdisciplinary research that integrates advanced ML techniques with technologies like blockchain, quantum-inspired optimization, and IoT-specific solutions. Ultimately, the research bridges critical gaps in IDS literature, addressing the research questions posed and contributing to the development of next-generation IDS equipped for the evolving cybersecurity landscape.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Lakireddy Bali Reddy College of Engineering (A), Mylavaram for providing the research facilities that were instrumental in completing this work. The resources and support offered by the center played a vital role in enabling the smooth progress of my research. I am deeply grateful to my supervisors, Dr. D. Veeraiah and Dr. L. Sumalatha, for their continuous guidance, invaluable insights, and unwavering encouragement throughout the course of this study.

DATA AVAILABILITY

This study is a review of existing datasets used for Intrusion Detection System using Machine Learning Methods, and no new datasets were generated or analyzed during the current study. The datasets referenced in this review are publicly available, and details about each dataset can be found in the respective studies cited throughout the paper.

REFERENCES:

[1] Alhajjar, E., Maxwell, P., and Bastian, N. (2021). Adversarial machine learning in network intrusion detection systems. Exp. Syst. Applic. 186:115782. doi: 10.1016/j.eswa.2021.115782

[2] Alenezi, N., and Aljuhani, A. (2023). Intelligent intrusion detection for industrial internet of things using clustering techniques. Computer. Syst. Sci. Eng. 46:36657. doi: 10.32604/csse.2023.036657

[3] Ali Hussein, A., and Boudour Ammar, M. C. B. B. H. (2024b). "Enhanced intrusion detection-based hybrid meta-heuristic feature selection," in 16th International Conference on Computational Collective Intelligence.

[4] Ali Hussein, A., and Maha Charfeddine, B. A. B. B. H. (2024a). "Intrusion detection schemes based on synthetic minority oversampling technique and machine learning models," in Conference 27th IEEE International Symposium on Real-Time Distributed Computing (IEEE).

[5] Alotaibi, A., and Rassam, M. A. (2023). Adversarial machine learning attacks against intrusion detection systems: a survey on strategies and defense. Fut. Internet 15:62. doi: 10.3390/fi15020062.

[6] Alzahrani, A. O., and Alenazi, M. J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. Fut. Internet 13:111. doi: 10.3390/fi13050111

[7] T. F. Lunt, R. Jagannathan, R. Lee, A. Whitehurst and S. Listgarten, "Knowledge-based intrusion detection," [1989] Proceedings. The Annual AI Systems in Government Conference, Washington, DC, USA, 1989, pp. 102-107, doi: 10.1109/AISIG.1989.47311.

[8] Mohit S D, Gayatri B K, Vrushali G M, Archana L G and Namrata R. B (2015). Using Artificial Neural Network Classification and Invention of Intrusion in Network Intrusion Detection System. International Journal of Innovative Research in Computer and Communication Engineering, 3(2).

[9] Zaman S, El-Abed M and Karray F (2013 January). Features selection approaches for intrusion detection systems based on evolution algorithms.

[10] Nazir A (2013). A Comparative Study of different Artificial Neural Networks based Intrusion Detection Systems. International Journal of Scientific and Research Publications, 3(7), 1-15.

[11] Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemal Ciliz, An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks, Expert Systems with Applications, Volume 29, Issue 4, 2005, Pages 713-722, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2005.05.002.

[12] Ambusaidi M A, He X Nanda P and Tan Z (2016). Building an intrusion detection system using a filter-based feature selection algorithm. IEEE transactions on computers, 65(10), 2986-2998.

[13] Varma P R K, Kumari V and Kumar S S (2016). Feature selection using relative fuzzy entropy and ant colony optimization applied to a real-time intrusion detection system. Procedia Computer Science, 85, 503-510.

[14] Thaseen I S and Kumar C A (2017). Intrusion detection model using a fusion of chi-square feature selection and multi-class SVM. Journal

of King Saud University-Computer and Information Sciences, 29(4), 462-472.

[15] Khammassi C and Krichen S (2017). A GA-LR Wrapper Approach for Feature Selection in Network Intrusion Detection. Computers & Security, 70, 255-277.

[16] Raman M G, Somu N, Kirthivasan K, Liscano R and Sriram V S (2017). An efficient intrusion detection system based on a hyper graph-Genetic algorithm for parameter optimization and feature selection in support vector machine. Knowledge-Based Systems, 134, 1-12.

[17] Zhu Y, Liang J, Chen J and Ming Z (2017). An improved NSGA-III algorithm for feature selection is used in intrusion detection. Knowledge-Based Systems, 116, 74-85.

[18] Aljawarneh S, Aldwairi M and Yassein M B (2018). Anomaly-based intrusion detection system through feature selection analysis and building a hybrid efficient model. Journal of Computational Science, 25, 152-160.

[19] Roshan S, Miche Y, Akusok A and Lendasse A (2018). Adaptive and online network intrusion detection system using clustering and extreme learning machines. Journal of the Franklin Institute, 355(4), 1752-1779.

[20] J. Hu, X. Yu, D. Qiu and H. -H. Chen, "A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection," in IEEE Network, vol. 23, no. 1, pp. 42-47, January-February 2009, doi: 10.1109/MNET.2009.4804323.

[21] McHugh, J. (2001). Intrusion and intrusion detection. International Journal of Information Security, 1, 14-35.

[22] Chen, T. M., & Venkataramanan, V. (2013). Dempster-Shafer theory for intrusion detection in ad hoc networks. IEEE Internet computing, 9(6), 35-41.

[23] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1), 1-22.

[24] Shafi, K., & Abbass, H. A. (2013). Evaluation of an adaptive genetic-based signature extraction system for network intrusion detection. Pattern Analysis and Applications, 16(4), 549-566.

[25] Koc, L., Mazzuchi, T. A., & Sarkani, S. (2012). A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier. Expert Systems with Applications, 39(18), 13492-13500.

[26] Adebowale, A., Idowu, S. A., & Oluwabukola, O. (2013). An overview of database centred intrusion detection systems. Int. J. Eng. Adv. Technol, 3(2), 273-275.

[27] Thaseen, S., & Kumar, C. A. (2013, February). An analysis of supervised tree based classifiers for intrusion detection system. In 2013 international conference on pattern recognition, informatics and Mobile engineering (pp. 294-299). IEEE.

[28] Rathore, M. M., Ahmad, A., & Paul, A. (2016). Real time intrusion detection system for ultra-high-speed big data environments. The Journal of Supercomputing, 72, 3489-3510.

[29] Bamakan, S. M. H., Amiri, B., Mirzabagheri, M., & Shi, Y. (2015). A new intrusion detection approach using PSO based multiple criteria linear programming. Procedia Computer Science, 55, 231-237.

[30] Aburomman, A. A., & Reaz, M. B. I. (2017). A survey of intrusion detection systems based on ensemble and hybrid classifiers. Computers & security, 65, 135-152.

[31] Horng, S. J., Su, M. Y., Chen, Y. H., Kao, T. W., Chen, R. J., Lai, J. L., & Perkasa, C. D. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. Expert systems with Applications, 38(1), 306-313.

[32] Jabbar, A. F., & Mohammed, I. J. (2020, November). Development of an optimized botnet detection framework based on filters of features and machine learning classifiers using CICIDS2017 dataset. In IOP Conference Series: Materials Science and Engineering (Vol. 928, No. 3, p. 032027). IOP Publishing

[33] Liao, X., Hao, D., & Sakurai, K. (2011, June). Classification on attacks in wireless ad hoc networks: A game theoretic view. In The 7th International Conference on Networked Computing and Advanced Information Management (pp. 144-149). IEEE.

[34] Chadha, K., & Jain, S. (2015). Hybrid genetic fuzzy rule-based inference engine to detect intrusion in networks. In Intelligent Distributed Computing (pp. 185-198). Springer International Publishing.

[35] Chaïri, I., Alaoui, S., & Lyhyaoui, A. (2012, September). Intrusion detection-based sample selection for imbalanced data distribution. In Second International Conference on the Innovative Computing Technology (INTECH 2012) (pp. 259-264). IEEE.

[36] Ambusaidi, M. A., He, X., Nanda, P., & Tan, Z. (2016). Building an intrusion detection

system using a filter-based feature selection algorithm. IEEE transactions on computers, 65(10), 2986-2998.

[37] Varma, P. R. K., Kumari, V. V., & Kumar, S. S. (2016). Feature selection using relative fuzzy entropy and ant colony optimization applied to real-time intrusion detection system. Procedia Computer Science, 85, 503-510.

[38] Thaseen, I. S., & Kumar, C. A. (2014, November). Intrusion detection model using fusion of PCA and optimized SVM. In 2014 International conference on contemporary computing and informatics (IC3I) (pp. 879-884). IEEE.

[39] Khammassi, C., & Krichen, S. (2017). A GA-LR wrapper approach for feature selection in network intrusion detection. computers & security, 70, 255-277.

[40] Raman, M. G., Somu, N., Kirthivasan, K., Liscano, R., & Sriram, V. S. (2017). An efficient intrusion detection system based on hypergraph-Genetic algorithm for parameter optimization and feature selection in support vector machine. Knowledge-Based Systems, 134, 1-12.

[41] Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, 152-160.

[42] Farooqi, A. H., & Khan, F. A. (2019, December). Intrusion detection systems for wireless sensor networks: A survey. In International Conference on Future Generation Communication and Networking (pp. 234-241). Berlin, Heidelberg: Springer Berlin Heidelberg.

[43] Zhang, Y., Wang, L., Sun, W., Green II, R. C., & Alam, M. (2019). Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Transactions on Smart Grid, 2(4), 796-808.

[44] S. Kumar, S. Gupta and S. Arora, "Research Trends in Network-Based Intrusion Detection Systems: A Review," in IEEE Access, vol. 9, pp. 157761-157779, 2021, doi: 10.1109/ACCESS.2021.3129775.

[45] Fu, B., Xiao, Y., Liang, X., & Chen, C. P. (2014). Bio-inspired group modeling and analysis for intruder detection in mobile sensor/robotic networks. IEEE transactions on cybernetics, 45(1), 103-115.

[46] Wei, P., Li, Y., Zhang, Z., Hu, T., Li, Z., & Liu, D. (2019). An optimization method for intrusion detection classification model based on deep belief network. Ieee Access, 7, 87593-87605.

[47] Yang, H., Li, T., Hu, X., Wang, F., & Zou, Y. (2019). A survey of artificial immune system based intrusion detection. The Scientific World Journal, 2014(1), 156790.

[48] Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network intrusion detection combined hybrid sampling with deep hierarchical network. IEEE access, 8, 32464-32476.

[49] Gu, G., Fogla, P., Dagon, D., Lee, W., & Skorić, B. (2021, March). Measuring intrusion detection capability: An information-theoretic approach. In Proceedings of the 2006 ACM Symposium on Information, computer and communications security (pp. 90-101).

[50] Ping, Y., Futai, Z., Xinghao, J., & Jianhua, L. (2021). Multi-agent cooperative intrusion response in mobile adhoc networks. Journal of Systems Engineering and Electronics, 18(4), 785-794.

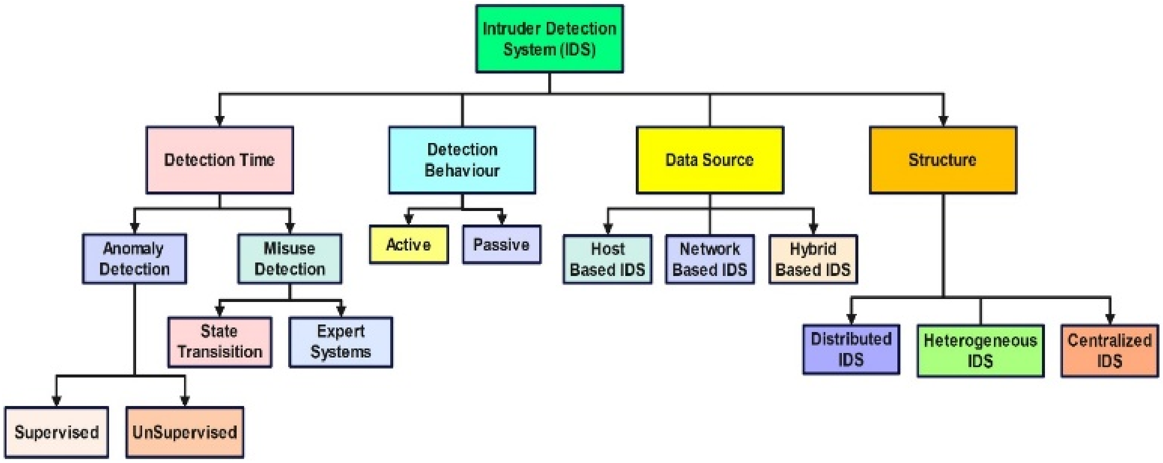

Figure 3: Classification of IDS

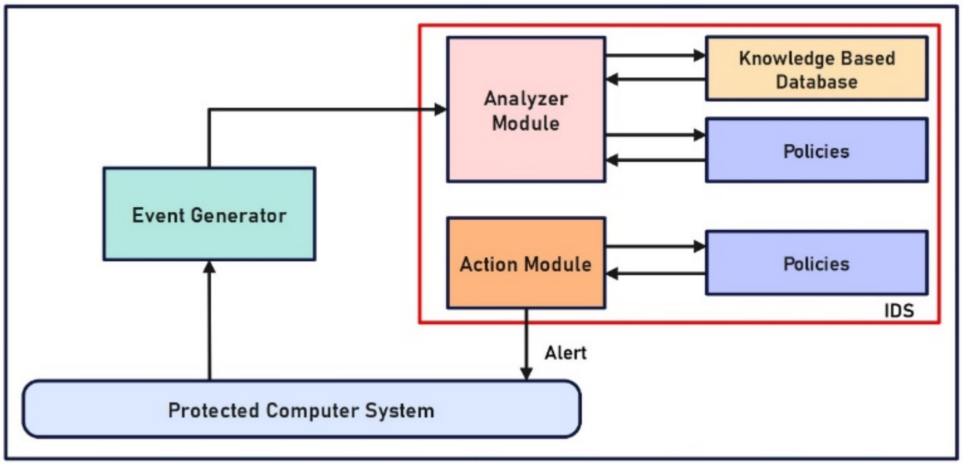

Figure 4: Knowledge-based IDS

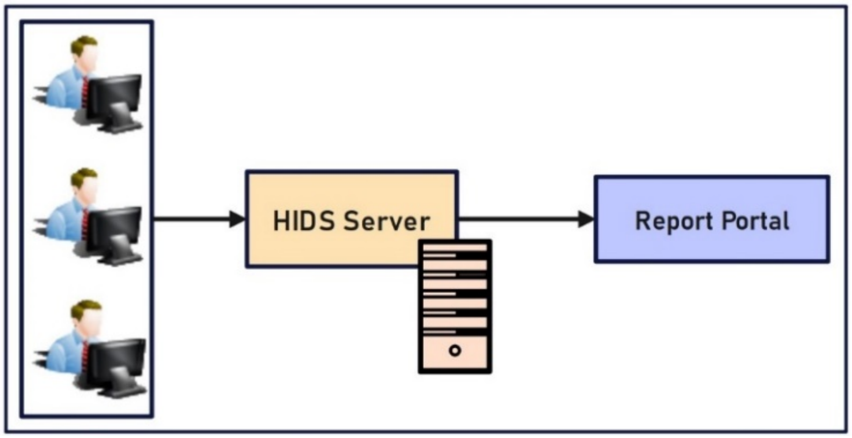

Figure 5: Host-based IDS

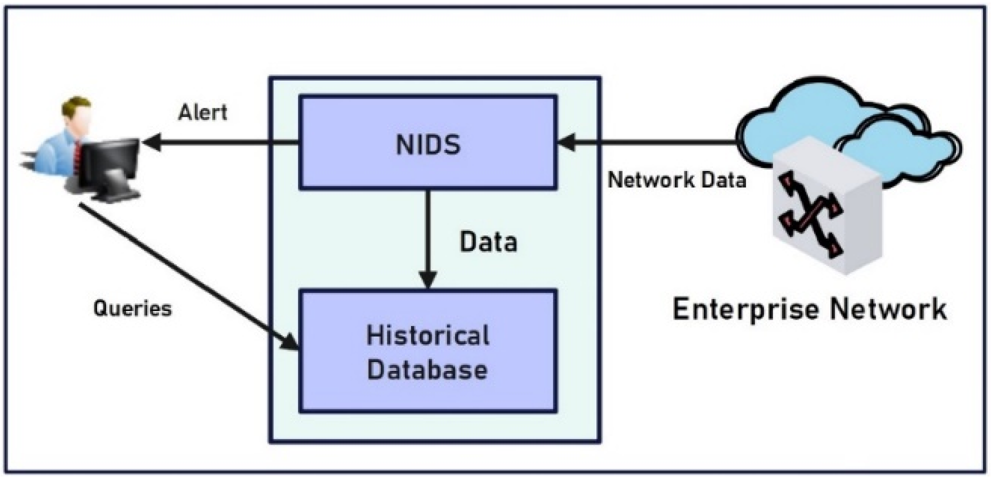

Figure 6: Network-based IDS

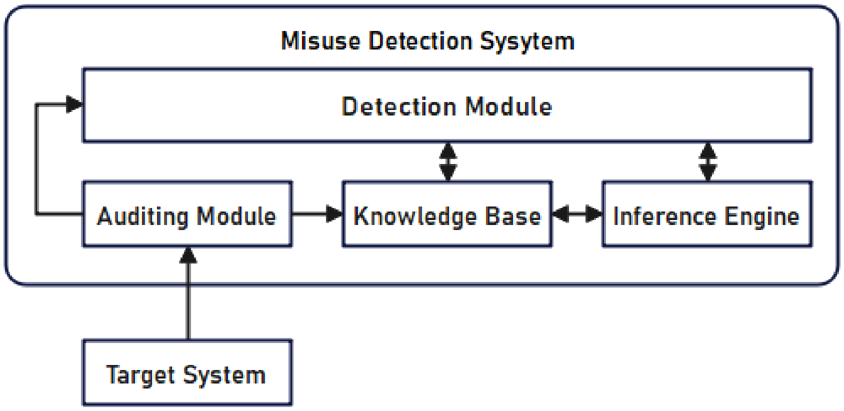

Figure 7: Misuse Detection Systems

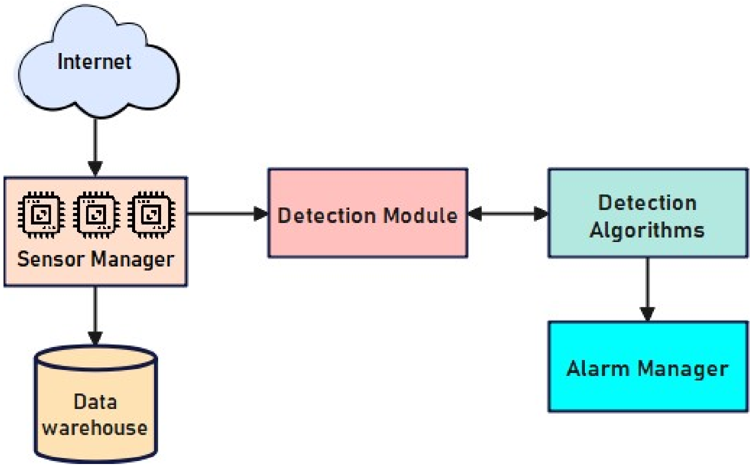

Figure 8: Architecture of Intrusion Detection System

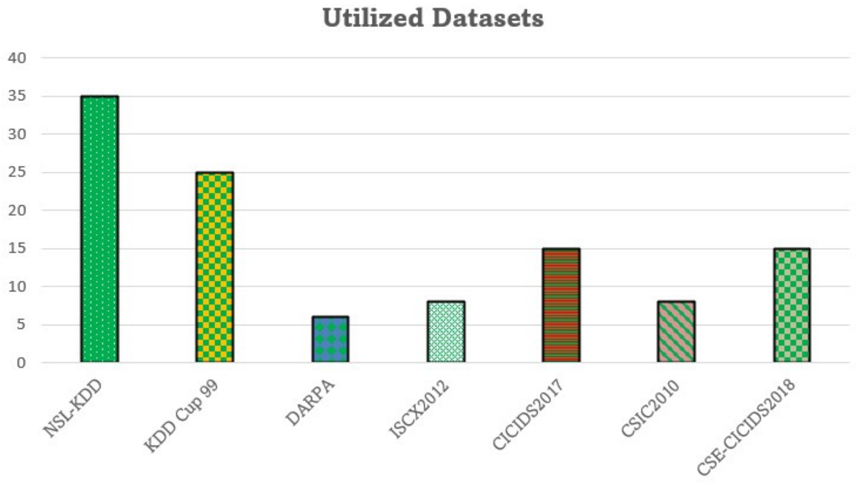

Figure 10: Utilized datasets in Various Models

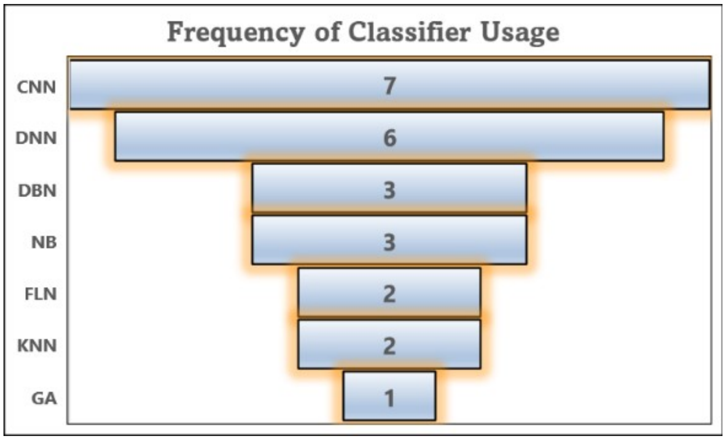

Figure 11: Percentage frequency of classifier used

s

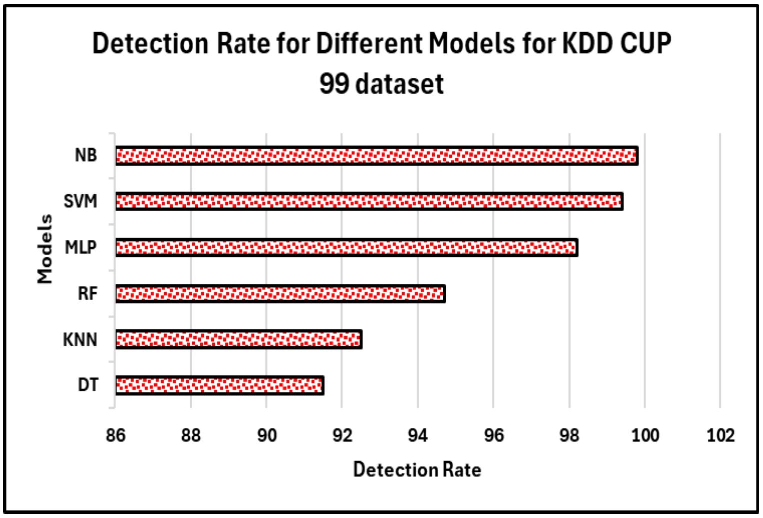

Figure 12: Detection Rate for Different Models for KDD CUP 99 dataset

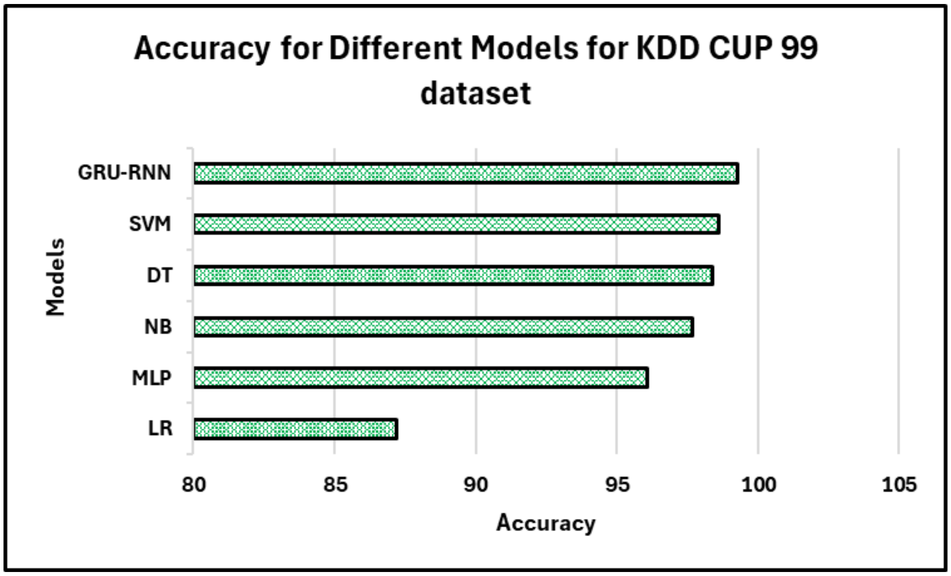

Figure 13: Precision for Different Models for KDD CUP 99 dataset

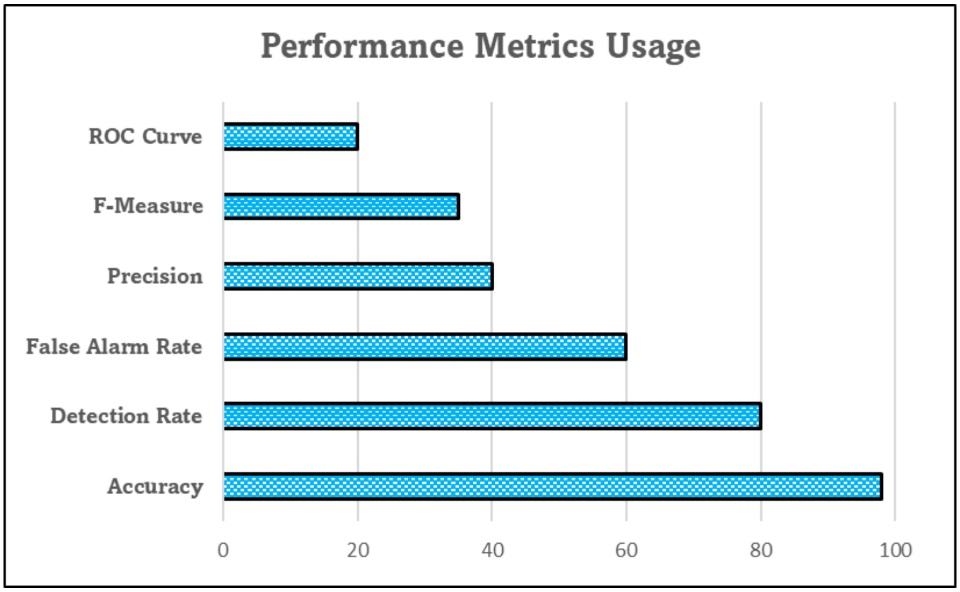

Figure 14: Percentage of performance metrics usage

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Attacks Category with Description

Attacks Category	Description	TCP/IP Layer
Probe	Surveillance and other probing	Transport Layer
Probe		Application Layer
R2L	Unauthorized admittance from a remote machine	Transport Layer
R2L		Application Layer
U2R	Unauthorized admittance to local super user (root) privileges	Application Layer
DoS	Denial-of-service (fake address generated)	Transport Layer
DoS		Application Layer

Table 2: Comparison of Existing Methods (Proficient = ✓, Incompetent = X)

Method	Statistical Anomaly-based IDS	Knowledge-based IDS	Hybrid-Based Approach
Pre-Knowledge or Rule	✓	✓	✓
Alert Reduction	✓	X	✓
Reducing False Alerts	✓	X	✓
Alert Prioritization	✓	✓	✓
Extract Attack Scenario	✓	✓	✓
Predict Next Alert	✓	X	X
Construct and Predict Attack	X	X	X

Table 3: Comparison of Outcomes from Different Approaches Using IDS Datasets

Reference	Dataset	Result	Observations
Hu, et al. (2009) [20]	DARPA 98	According to Snort's detection, false alarms account for 69% of all produced alerts.	SIDS is used in the absence of AIDS
McHugh (2001) [21]		The DR ("Detection Rate") of ANN analysis procedure is 96%.	An ANN ("Artificial Neural Network") classifier has been utilized to formulate and investigate the framework.
Chen, et al. (2013) [22]		A subset of DARPA 98 with a 99.6% DR was used for SVM.	SVM is capable of handling multidimensional data and divides it into distinct classes with a hyperplane or hyperplane.
Khraisat, A et al .[23]	KDDCUP 99	90% DR using multivariate statistical study of audit data	Multivariate analysis lowers the incidence of false alarms.
Shafi and Abbass (2013) [24]		C4.5 method, which achieves a 95% TPR (True Positive Rate), has produced best results.	C4.5's decision trees may be applied to categorization tasks.
Shafi and Abbass (2013) [24]		SMO classifier with a 97% DR	This SMO-implemented SVM-based classifier yields high detection accuracy. However, because the dataset of KDDCUP 99 is more intricate and extensive than the dataset of DARPA 98, the reported accuracy is lower than that of Chen et al. (2005).
Koc, et al. (2012) [25]		The HNB model is the most effective model when comparing the models with a 95 percent confidence level.	In terms of IDS detection accuracy, the HNB strategy performs better as compared to the base on the conventional NB technique.
Adebowale, et al. (2013) [26]	NSL-KDD	The k-NN (K-Nearest Neighbor) method has a 94% DR.	Every labelled training instance is used as a model of the target function by the k-NN method. In the classification stage, k-NN finds a local optimum hypothesis function by applying a similarity-based search technique.
Adebowale, et al. (2013) [26]		The DR using NB is 89%.	Bayesian classifiers offer mediocre accurateness since emphasis is on identifying classes for cases rather than the precise probability.
Thaseen and Kumar (2013) [27]		99 percent was the best DR provided by C4.5.	To increase accuracy, C4.5 chooses the data characteristic that splits its collection of samples into subgroups the most effectively.
Adebowale, et al. (2013) [26]		SMO classifier, with a 97% DR.	The study obtains a DR comparable to using an SVM-based classifier (Chen et al., 2005).
Ahmed, et al. (2016) [28]		Clustering using EM ("Expectation Maximization") has a 78% accuracy rate.	Each row is given a "soft" task by EM, which divides it into several groups according to the likelihood of each group. The precision of this method is constrained as EM does not offer a parameter covariance matrix for standard errors.

Table 4: Comparing Accuracies of Datasets on Different Attacks

Authors	Used Methods	Types of Attacks	Datasets	Accuracy
Bamakan et al. (2015) [29]	K-Means + KNN	DoS, Probing Attack, R2L (“Remote to Local”) and U2R (“User to Root”)	KDD-Cup 99	93.55
Aburomman et al. (2017) [30]	SVM+KNN+PSO			88.44
Horng. et al. (2011) [31]	HC+SVM		KDD-Cup 99 DARPA	95.72 69.82
Jabbar. et al. (2020) [32]	RF+AODE	Various attacks against honeypots	Kyoto	90.51
Liao. N. et al. (2011) [33]	FL+ES	DDoS, DARPA attacks	DARPA 2000	91.51
Chadha. K. et al. (2015) [34]	FL+GA	DoS, U2R, R2L and Probing Attack	KDD-Cup 99 DARPA	94.62

Table 5: Comparison of Merits and Demerits of Different ML Methods Based IDS

Authors	Methods	Merits	Demerits	Performance Metrics
Chaïri I. et al. (2012) [35]	Sample Selection Method, MLP	The process of choosing samples enhances performance through the application of the sample selection method.	The several layers of computing units of MLP result in a significant processing cost.	Precision = 97.2%

Ambusaidi M A. et al. (2016) [36]	“Filter-based feature selection technique, FMIFS LSSVM-IDS	Minimal computational expense	The dataset has an unbalanced sample distribution.	FPR = 0.28,
				DR = 98.7%
				Accuracy = 99.9%

Varma P R K. et al. (2016) [37]	Fuzzy entropy-based heuristics, ACO	A quick and easy method of identifying intrusions.	The ACO's time to convergence is unknown.	Mean accurateness = 99.5%
Thaseen.I S. et al. (2017) [38]	SVM multi-class, Chi-square feature selection	Extraordinary classification accurateness	It is more challenging to choose the kernel function correctly in SVM.	Accuracy = 95.8%

Khammassi C. et al. (2017) [39]	Logistic regression Genetic	Good DR	failed to extract the best selection of features to improve classification	FAR = 0.105
				DR = 99.8%
				Accuracy = 99.9%

	algorithm, RF, NB Tree, C4.5		precision and reduce cases of misclassification	

Raman.M G. et al. (2017) [40]	HG-GA, SVM	High DR	SVM is limited in terms of size and speed.	Accuracy = 96.7%
				DR =97.1%
				FAR = 0.83

Aljawarneh S. et al. (2018) [41]	Hybrid model, REPTree, AdaBoost, NB, Meta Bagging, and Random Tree	Minimize time complexity	A completely dispersed network will not be supported by it.	Accuracy = 99.2%

Khan F A et al. (2019) [42]	Novel 2-stage DL model	High recognition rate	An uneven distribution of classes has an impact on learning effectiveness.	Accuracy = 99.9%
				FAR = 0.00001%

Zhang Y. et al. (2019) [43]	Enhanced GA, DBN	A high rate of recognition makes the network structure less complicated.	Enhance time of detection	Precision = 9.20%
				Accuracy = 99.4%

Xiao Y. et al. (2019) [45]	Feature reduction method, CNN	enhances the performance of categorization	Ineffective for a limited range of attack types	DR = 0.96
				Accuracy = 97.1%

Zhang Y et al. (2019) [43]	LSTM, LeNet-5 Neural Network	Superior accurateness	To identify unidentified and untrained attack types	Accuracy = 99.1%
				Precision = 99.3%

Wei P. et al. (2019) [46]	DBN, PSO	Lowers typical detection time	It significantly affects training time	Accuracy = 83%
				FPR = 0.77%

Yang H. et al. (2019) [47]	DBN, SVM, RBM	Effectiveness of intrusion detection	It is not more effective When the network intrusion type's sample size is small.	Precision = 97.2%
				Accuracy = 97.4%

Jiang K. et al. (2020) [48]	Network intrusion Detection algorithm, CNN, OSS, BiLSTM, SMOTE	superior recall, accuracy, and precision performance	Superior Training time”	Precision = 80.8%
				Accuracy = 80.1%

Gu et al. (2021) [49]	SVM model using NB	On 2 recent datasets, CICIDS2017 and UNSW-NB15, an SVM model with excellent accuracy outcomes uses NB for feature selection.	Type of attack that is being employed is not specified in their answer.	Accuracy = 98.92%
				Accuracy = 93.75%

Yiping et al. (2022) [50]	Random Forest Mode	A wireless network concept based on random forests.	A mean accuracy of 96.93 percent was attained. There was no usage of known datasets.	Accuracy = 96.93%.