FUW CENTRE FOR RESEARCH JOURNAL OF SCIENCE AND TECHNOLOGY (FUWCRJST)

Intrusion Detection and Prevention Systems: A Systematic Reviewed

[1]Abraham Danlami., [2]Etemi Joshua Garba & [3]Yusuf Musa Malgwi

[1]*Federal University Wukari, Taraba State*

[2&3]*Department of Computer Science, Taraba State University*

Corresponding Email: *abrahamdanlami@fuwukari.edu.ng*

Abstract

The Intrusion Detection and Prevention System (IDPS) is a system that monitors a network for any threats and takes the necessary steps to neutralize them. Cyberattacks compromise the security, integrity, and availability of data and make it more difficult to detect intrusions. These review papers offer a thorough examination of popular assessment datasets, the most recent IDPS taxonomy, and intrusion detection technologies. It discusses how to strengthen network security by understanding how attackers employ evasive techniques and how challenging it is to stop them. Researchers strive to enhance IDPS by precisely identifying intruders, reducing false positives, and identifying emerging threats. Machine learning (ML) and deep learning (DL) techniques are used by IDPS systems, and they are capable of effectively detecting network intrusions. This paper looks at the methodology, evaluation criteria, and dataset selection of the most current advancements in deep learning (DL) and machine learning (ML)-based network intrusion detection systems (NIDS). It identifies research bottlenecks and proposes a future research paradigm to solve the methodology's inadequacies. This study aims to provide insight into the process of developing an effective detection framework for decision trees. Based on the combination of results from a comparative survey, the decision tree which is recognized for its speed and ease of use is proposed as a model for identifying abnormalities in results. In my view, this systematic review study provides a road map for IDPS-focused academics and business personnel.

Keywords: Intrusion Detection, Prevention System, Systemic Review, Technologies

Introduction

The Internet has become into a useful tool and a component of everyday life. In many areas of human life, such as business, education, and entertainment, it happens. According to Shon et al. (2024), it is an essential component of working in business. To put it another way, we use networks more and more in every aspect of our lives as technology advances. As network usage grows in popularity, so do the risks of a network attack Shon et al., (2024).

The Internet has become into a useful tool and a component of everyday life. In many areas of human life, such as business, education, and entertainment, it happens. According to Shon et al. (2024), it is an essential component of working in business. To put it another way, we use networks more and more in every aspect of our lives as technology advances. As network usage grows in popularity, so do the risks of a network attack Ethala et al., (2013) noted an increase in interest in alternative security solutions like intrusion detection systems (IDSs). Intrusion detection systems (IDSs) monitor computer networks, searching

for hostile activity such as censorship, data theft, or protocol breaches.

The majority of intrusion detection systems (IDSs) currently in use are unable to handle the complex and dynamic nature of cyberattacks on computer networks; as a result, the network security solutions currently in use are still insufficient to secure computer systems due to the daily evolution of these harmful attacks. As a result, it is imperative to develop new techniques and advance existing technology in this area. This study aims to conduct a detailed analysis of IDSs, existing development methodologies, available datasets, and unresolved issues. In the literature Biermann et al. (2020), intrusion detection technologies, approaches, frequently used tools, and cutting-edge techniques are carefully studied for this aim.

The current status of IDPSs is investigated and examined in this research (Ethala et al., 2013) by a thorough and comprehensive examination of the literature. First, an overview of the key elements of an IDPS is provided, along with a description of the system's objectives. Then, IDSs are categorized according to how they monitor network activity, record flow data, spot intrusions, and send out alarms. All IDS technologies, methodologies, and approaches included in this scope have been thoroughly examined an extensive overview of the work done in each field is given, along with a breakdown of the benefits and drawbacks of each. Then, a study was done on the datasets that are commonly used in the testing and evaluation phase of the constructed intrusion detection systems, and these datasets were thoroughly described. Finally, common intrusion detection tools that people, organizations, and groups use to find attacks are mentioned. The benefits and drawbacks of each intrusion detection and prevention tool's methodology are examined.

This review paper is not like the previous survey publications in many aspects. Previous studies have mostly focused on one or two subjects, like the intrusion detection and prevention datasets or methodologies. Conversely, the many IDS features are covered in this study. Furthermore, for each issue, many recommendations are being provided. Furthermore, the study assists corporate organizations looking to enhance their use of IDPSs as well as academics.

The contributions of this study are summarized below:

a) In this context, new technological breakthroughs and the current state of intrusion detection systems are explained.
b) A synopsis of recent research in these fields is provided, along with an explanation of intrusion detection technologies, methodology, and approaches.
c) New hypotheses for intrusion detection systems are put out, and current difficulties and issues are examined.
d) Offers a methodical synopsis of intrusion detection and prevention systems and techniques for more research.

e) The focus of this paper is to review the systematic literature concerning the architectural development of IDPS with a special emphasis on the distributed control and programmability of sensor nodes.

The following questions are the formulated guide to this research to address its aim:

I. What are the potential in efficiently detecting intruders across networks?
II. What are the Intrusion Detection Technologies?
III. What is the conceptual research studies conducted in the field of IDPSs?

The structure of the paper is as follows. Section II provides an overview of IDPS systems, while Section I reviews the literature on IDPSs to provide a compelling case for the study. Section III provides an explanation and evaluation of studies and technology related to intrusion detection. Section V provides an explanation of intrusion detection approaches, while Section IV provides intrusion detection methodologies. Furthermore, Section V also includes an evaluation of recent findings. Frequently used datasets are reviewed in Section VI. Currently available, well-known IDS tools are examined in Section VII. A general assessment and an IDS comparison are provided in Section VIII. Section IX concludes with recommendations for further research.

Existing Review Studies and Motivation

Review articles already published by Ahmed et al. (2016), Buczak and Guven (2016), Axelsson et al. (2015), and Azhagiri et al. (2015) The focus of Lu et al. 2020, Agrawal and Agrawal, (2016) and Zahedi et al. 2023 is on techniques for preventing intrusions, dataset problems, certain kinds of cyberattacks, and IDPS evasion. An update is required because, as these systems have evolved, several alternative designs for intrusion-detection systems have been created in the interim. This paper describes the new taxonomy of the intrusion-detection discipline, which further enhances the taxonomies offered by Azhagiri et al. (2015) and Zahedi et al. (2023).

The only study that provides a thorough overview of the developing IDPSs and provides a brief explanation of dispersed IDPSs is Malek et al., (2020) study. Our study indicates that one of the earlier survey publications that offer insights into IDPS is the work done in 2013 by Liao et al. The majority of the study focuses on IDPSs and whether or not IPS is appropriate for use with mobile and wireless networks. A particular emphasis on the IDPSs is given by Aslan et al., (2020) Samet, however reference Malek et al. (2020) goes beyond that. For example, the paper starts out with a synopsis of the IDS concept before making certain promises and skipping over some of the IDPSs' fundamental issues. Relevant networking concepts are also looked at in order to establish a connection

between the two paradigms (IPSs and IDSs) and their networking feasibility. This study shows even further how IDS can be used to solve problems that IPSs encounter. Additionally covered are significant IDPS subjects like design, routing, network administration, security, and standards. Finally, the study examines the several controller implementations used in IDPSs, including distributed and single controllers. Following a succinct explanation of the two concepts, their differences are ascertained. Lastly, a range of concepts and approaches, applications and structure, issues and challenges are provided. Additionally, citation While Qureshi et al. (2018) provides a thorough examination of distributed controllers and their classification based on the IDS concept, they do not discuss or make reference to IDPSs in their work. The paper first discusses several controllers before analyzing their features in terms of performance, languages, and applications. Furthermore, the Biermann et al., (2021). Research categorizes literature-based suggestions and lists technologies that make it possible to integrate 5Gs with the IDPS paradigm. Moreover, a new article by Riyaz et al. (2020), which also assesses energy-saving strategies, presents an updated and comprehensive IPS evaluation as an energy optimization technique.

Table 1 presents the synopsis and main points of several relevant review articles. A synopsis of the review articles that were released as conference papers as a component of the research is shown in Table 3. It's interesting to observe that, in addition to a few other areas like machine learning, topology, data aggregation, etc., the majority of articles focus on security challenges. Figure 1 displays the categorization of the various IDPS themes that have been studied in the literature. To the best of our knowledge, no research has focused exclusively on the distinctive dispersed aspect of IDPSs, especially its cutting-edge architectural advancement, aside from the analysis of the various IDPS applications and the distributed IPS control logic found in literature. The systematic literature review (SLR) review approach is a tried-and-true technique for reducing bias in the literature and providing information and evidence about both consistent and inconsistent findings over a wide range of prior studies, however it is not used in any of the current investigations Aldwairi et al., (2017). Thus, this work focuses specifically on the architectural development of IDPSs from the perspectives of software Security, programmable Security nodes, and the distributed control logic of IDPSs. The section that follows discusses the review process employed in this study.

Research Methodology

The study explores ML and DL-based NIDS and decision tree approaches in detail through an examination of published journal articles. Keele et al., (2020) employ a systematic literature review process to collect and evaluate relevant data on the topic. This systematic review has two steps, as indicated below:

Table1: Critical analysis of the existing review on the relationship between Intrusion Detection and Prevention System

Paper//Year	Proposed Method	Goals/Success/Focus
Mudzingwa and Agrawal, (2012)	A detailed review of main techniques using intrusion detection and prevention systems.	Anomaly-based technique is superior to other techniques, but most of the IDPS use a combination of the main methodologies.
Seo et al., (2013)	A tasteful Intrusion prevention inspection mechanism called SIPAD.	The proposed approach significantly reduces the operating cost. It can be used even in resource-constrained environments such as smartphones.
Yang et al., (2014)	A stateful Intrusion Detection System that uses the Deep Packet Inspection method.	A proposed approach specifically designed for the IEC 60870-5-104 protocol. The new intrusion detection approach has been tested and validated.
Kang et al., (2016)	A framework for detecting smart grid attacks.	The attacks that can create dangerous situations can be detected effectively.
Boite et al., (2017)	The stateful Intrusion Detection System paradigm is named State.	StateSec detects and mitigates various attacks such as DDoS and port scans with high accuracy.
Lewis et al., (2018)	A filtering approach named as P4ID.	This system was evaluated by combining the CICS2017 dataset and the Emerging Threats rule set. A significant reduction in traffic handled by IDS can be achieved.
Sharma et al., (2019)	A lightweight behavior rule specification-based misbehavior detection and prevention for the IoT-embedded cyber-physical systems (BRIoT).	The proposed approach is verified by an embedded system in an embedded system in an unmanned aerial vehicle. The feasibility of the proposed model is demonstrated with high reliability, low operational cost, low false-positives, low false-negatives, and high true positives in comparison with existing rule-based solutions.
Rashid et al., (2020)	A comprehensive and comparative analysis of the NSL-KDD and CIDDS-001 datasets.	KNN, SVM, NN and DNN classifiers have approximately 99% accuracy in the k-NN and Naïve Bayes classifiers CIDDS-001 dataset.
Sbai and Elboukhari, (2020)	An IDS using deep neural network technology to detect the subclass of the big class DDoS: Data flooding attack.	The proposed model evaluated on the dataset CICDDoS2019. The obtained results show that the proposed architecture model achieves interesting performance

		(Accuracy, Precision, Recall and FI-score).
Choudharry and Kesswani, (2021)	A hybrid classification approach to detect multi-class attacks in the IoT network.	The 81.02% detection rate, 2.22% false alarm rate and 92.85% detection rate, 2.99% false alarm rate were obtained respectively on UNSW-NBI5 and NSL-KDD dataset.
(Alsubaei, 2023)	Detection and Prevention of Inappropriate Tweets Linked to Fake Accounts on Twitter	A reactive system, does not proactively preempt social media user of the fake account.
Hami et al., (2024)	Detection methods in HIDSs were emphasized, and investigated	The balance of detecting attacks with both high ACC and low FAR values was not achieved by HIDSs or IDPSs

Table 2 Critical analysis of the existing review on the relationship between Intrusion Detection and Prevention System

Related work Paper and Year	IDS	IPS	IDPS
Mudzingwa and Agrawal (2012)			✓
Seo et al. (2013)	✓		
Yang et al. (2014)		✓	
Kang et al. (2016)	✓		
Boite et al. (2017)	✓		
Lewis et al. (2018)		✓	
Sharma et al. (2019)			✓
Rashid et al. (2020)	✓		
Sbai &Elboukhari, (2020)	✓		
Choudharry and Kesswani, (2021)	✓		
(Alsubaei et al., (2023)			✓
Hami et al., (2024)			✓

A) Intrusion Detection Prevention System (IDPS) DIAGRAM

As demonstrated below, an intrusion detection and prevention system (IDPS) keeps an eye on a network for potential threats and notifies the administrator in order to stop potential attacks:

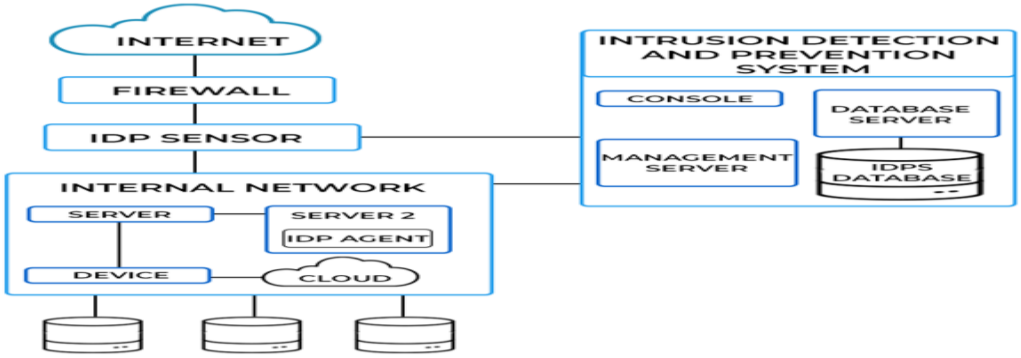

Fig.1: IDPS (Keele et al., 2020)

As the above diagram shows, a firewall is the first line of defense against unsolicited and suspicious traffic entering a system. It is simple to think that no malicious traffic can get past firewalls and onto the network. However, thieves are always coming up with new strategies to evade security measures. In this case, an intrusion detection and prevention system can be useful. A firewall regulates what enters the system, whereas the IDPS manages what goes through it. Often, it cooperates with the firewalls right behind them.

The operation of an intrusion detection and prevention system is comparable to that of airport security and baggage claim. Travelers must provide their ticket or boarding permit when they enter an airport, and they are not allowed to board the aircraft until after completing all required security procedures. In a similar vein, an intrusion detection system (IDS) simply monitors harmful traffic or rules violations. It was the precursor to the intrusion prevention system (IPS), also known as the intrusion detection and prevention system. The IPS uses automated actions to try to prevent such events in addition to monitoring and alerting users (Aldwairi et al 2017).

Evaluation of Quality

The quality of the papers was assessed using a number of criteria, some of which were proposed in Ethala K. et al. 2013, Keele et al 2020, and Riyaz et al 2020. On the other hand, 23 evaluated every manuscript independently using the indexed IF journal. We have determined that the publications from IEEExplore, Springer, and Science Direct meet the quality assessment standards that were applied during this inquiry. Furthermore, documents from Google Scholar that were free of duplicates were evaluated using the standards set by Riyaz et al 2020. The reliability of the selected sources was verified using the quality assessment rating criteria. In general, the elements of an efficient and successful intrusion detection system (IDS) are users, sensors, database servers, management servers, and networks, when it is necessary to firmly secure components. It is essential to safeguard these components because attackers aim to prevent IDSs from accessing known vulnerabilities, critical data, or attack detection.

All operating systems and programs must be up to date, and all software-based IDS components must be protected from threats. To provide accurate and comprehensive attack detection, using multiple IDS systems may also be an option. There are various IDS technologies in use, such as host-based, wireless, and network-based. They are all basically different in their abilities to capture, stop, and collect data. Benefits of each technology include improved efficiency or accuracy in recognizing particular events. One successful approach, for example, is to combine intrusion detection systems that are network-based and host-based. Stated differently, it is crucial to consider the many attributes and advantages of every intrusion detection system prior to making a choice. The most widely used intrusion detection system technologies, approaches, and methods in the literature are listed in Figure 1.In conclusion, intrusion detection systems (IDSs) are becoming a crucial part of almost every person, institution, and organization's security due to the rising reliance on technology and information systems, the spread of attacks, and their potentially dangerous outcomes.

IDS/IPS Security

Some companies pair firewalls and routers with IPS/IDS. The primary distinction between the two is that the firewall basically only checks the IP address and port number. Using the IP address and port number, traffic is blocked. It uses specific signatures for detection; a packet is transmitted if it complies with the conditions or recommendations listed in the signatures, and blocked otherwise.

Principles of IDPSs

Infiltration detection is the process of keeping an eye on and assessing events that occur within a computer system or network to find instances of infiltration. A few of the risks include malware, DoS-DDoS attacks, unauthorized access, privilege escalation, and probing assaults. The majority of occurrences that appear to be damaging to the system are really attacks, with very few exceptions. For example, a person can inadvertently connect to the wrong network or type the computer's address wrong. Accurate classification of intrusions from normal network traffic is required by the system. In conclusion, software that facilitates and automates the process of discovering attacks is known as an intrusion detection system.

There are some important factors for an effective attack resolution when applying IDPS technologies:

a) System durability/reliability;
b) Fast detection;
c) Minimal false positives;
d) Maximum detection rate;
e) Usage minimum software/hardware;
f) Ability to accurately detect the location of intrusion;
g) Ability to work with other technologies.

In summary, an IDPS must provide the above-mentioned features for high accuracy and timely detection of attacks.

Table 3. Confusion matrix.

		Prediction	
		Positive	Negative
Actual	Positive	TP	FN
	Negative	FP	TN

II) Basic Functions Of IDPSs

To begin with, the types of attacks that various IDPS technologies can identify and the methods by which they do so vary greatly. All forms of IDPS must have the previously listed functionality in addition to the capacity to watch and analyze events in order to identify undesired events.

A) Recording Information

Usually, data is kept locally to make comparisons or create pre-made profiles. Moreover, the recorded data is sent separately to central recording servers, information security solutions, and management systems.

B) Identification of Important Events

It is crucial to identify an event that differs from the data that is regularly recorded and considered typical as soon as possible.

C) **Notification of Identified Important Events**

These messages—also referred to as alerts—are delivered through a number of channels, such as emails and messages shown within the user interface of the system. A notice usually contains some basic information about suspicious incidents that have occurred. System users must contact the IDPS for additional information.

D) Generating Reports

The generated system reports can provide an in-depth description of significant occurrences or a synopsis of events that are seen. For example, if IDS detects suspicious activity throughout the session, it has the ability to collect more precise data. It can also change parameters, including when alerts should be sent out after a threat is detected.

The primary similarity throughout IDPS types is their incapacity to produce a completely precise detection. When an IDPS perceives a normal action as an attack, this is known as a false positive. A false negative will result if it is unable to detect and identify hostile conduct as usual. It is not possible to get rid of all of these false positives and negatives. As a matter of fact, when one goes down, the other usually goes up. Many IDPS developers would prefer to reduce the false negative rate even when the false positive rate increases.

III) Evaluation Metrics OF IDPSs

In general, metrics like recall, false positive, false negative, precision, f-measure, and accuracy are used to assess established IDS models and compare their performance. To compute these values, the confusion matrix is used in Table 2.

Recall = TP/(TP + FN)----------(1)

Precision = TP/(TP + FP)----------(2)

F-Measure = (2 ∗ precision ∗ recall) (precision + recall) ----------(3)

Accuracy = TP + TN/(TP + TN + FP + FN)----------(4)

An accurate forecast of the positive class (i.e., both the prediction and the actual are positive) is known as a true positive (TP). An accurate forecast of the negative class (when the fact and the prediction are both negative) is called a true negative (TN). A false positive (FP) is the inaccurate prediction of the negative class (actual: negative, predicted: positive). An inaccurate prediction of the positive class (really positive, expected negatively) is known as a false negative (FN). Precision, also called positive predictive value, is the ratio of relevant samples among the taken samples; recall, also called sensitivity, is the ratio of relevant samples taken. The F-measure is the harmonic mean of recall and precision. The metric that indicates the proportion of data that was successfully classified is called accuracy.

IV) Challenge of IDPSs

Security systems called intrusion detection systems monitor network traffic and computer systems to look for dangers such as system abuses, internal and external attacks, and other issues. Scarfone & colleagues, 2007. IDSs are currently thought to be among the essential security tools that companies need to use. IDPSs can be used as part of a tiered security architecture in conjunction with other security technologies. For example, many use IDPSs in addition to firewall and antivirus software. Therefore, IDPSs can be used to recognize attacks that other security products are unable to recognize.

IDPSs use a range of approaches and techniques to recognize attacks. Research on using system calls to identify anomalies has been done for a very long time. However, there remain gaps in databases that should ideally reflect all common acts, even after great attempts to develop universal datasets. Furthermore, anomaly-based techniques can categorize routine actions as attacks and can distinguish between known and unknown attacks to some extent. It is recommended that system administrators or end users investigate the behavior that IDPS classified as an attack. As a result, it is possible to recover the right signature of the program. After an examination, the application was determined to be an attack, and it was demonstrated that anomaly detection systems had detected it. Conversely, signature-based systems can recognize known attacks by their signature, but they are unable to recognize unannounced attacks. The field of machine learning techniques for intrusion detection has seen a surge in interest recently. Various classification techniques have demonstrated potential in addressing a broad spectrum of problems, such as pattern identification, image processing, and cyber security—specifically in the domain of intrusion detection. However, machine learning techniques are more useful when attempting to predict between two likely outcomes—normal or abnormal—for a given network traffic. The IDPS design

enables network programming by separating the data plane from the control or management plane and using centralized control. All network devices may be managed and monitored from a single central location. Centralized administration over IDP can improve and save processing and storage. However, IDPS does not have any standard security procedures. Even with some third-party service providers present, there is still a security risk. In conclusion, the present IDPSs are unable to handle the dynamic nature of the assault types that are evolving. References: Aleesa et al. 2020, Ozkan-Okay et al. 2020, Hadem et al. 2021, Kruegel et al. 2004, Han et al. 2014, Santos et al. 2014, García Teodoro 2009.

The research that is conducted in these areas should incorporate new technology, new dataset creation, and new approaches that will contribute to the body of literature. Another issue is that hybrid IDPSs, which combine the benefits of many IDPS types to offset each other's drawbacks, should be created in real-world scenarios. This study included a comprehensive evaluation and analysis of the types, advantages, and disadvantages of the IDPS in order to facilitate the creation of new technologies.

Results

The research questions determine the order of the study's conclusions. A brief explanation has been given for this study problem in an effort to give the most precise response.

Answers to Research Questions

Research questions 1-3 are addressed in this section in order to look at the studies from different angles.

Q1. What are the potential efficient detecting intruders across networks?

I) Network-Based IDPSs

A network-based IDPS (NIDS) monitors network traffic and looks into the protocols (network, application, transport, etc.) that have been used to identify suspicious activities in order to guarantee the security of the network devices Vigna et al. (2016). TCP/IP is a widely used protocol for network communication. TCP/IP consists of four interconnected layers. Every layer adds fresh information, and when a user wants to transfer data, it is transferred from the top layer to the bottom layer. After being communicated across the physical network by the lowest layer, the data is moved from the layers to the destination. The four TCP/IP layers work together to facilitate the transfer of data between hosts. In network-based intrusion detection systems, the application layer is where most analysis usually takes place. Limited hardware layer analysis is also performed by certain network-based intrusion detection systems. Network-based IDPSs usually include many consoles, database servers, and one or more administration servers. Every item on the list—aside from the sensors—is also found in other IDS technologies. Intrusion detection systems (IDS) that are based on networks monitor and analyze network activities.

II) Security Features Of NIDS

Network-based intrusion detection systems (IDSs) offer an abundance of security capabilities. The following

provides a thorough explanation of typical security features, which can be roughly divided into three groups: obtaining, logging, and identifying information.

a: Information Collection

Network-based intrusion detection systems are limited in their capacity to gather information from communication networks. In general, information about connected hosts and network activities is obtained. A summary of some of the characteristics of the data that was acquired is provided below.

i). Identifying Hosts: A list of network hosts can be generated by an IDS.

ii). **Identification of Operating System**: Hosts' operating systems and versions can be recognized. Identification of susceptible hosts can be aided by knowing the version of the operating system being utilized.

iii). **Identification of Applications**: By keeping an eye on open ports and application communication, an IDS sensor can detect the versions of applications. This data is utilized to pinpoint applications that may be weak points and their improper usage.

iv). **Determining Network Characterization:** Data is gathered on traffic, network setups, and general information about some IDS sensors. This information makes it simple to identify any modifications made to the network settings.

.b: Logging

IDSs based on networks log extensive information about events they notice. Investigating, correlating, and validating alarms are all done using this data. Typically, network-based intrusion detection systems log the following sorts of data:

- Date and time;
- Number of connections;
- Event type;
- Protocols;
- Source and destination IP addresses;
- Number of transmitted packets;
- Application requests and responses.

c: Detection

Network-based IDSs provide a wide range of detecting powers. To carry out in-depth analysis and boost the detection rate, many network-based intrusion detection systems incorporate anomaly- and signature-based techniques. The anomaly-based approach analyzes aberrant activity by parsing it into requests and answers, which are then scrutinized and contrasted with the known attack signatures. In other words, the methods' implementation is hierarchical..

III) Related Work

Network-based intrusion detection systems (IDSs) offer a variety of detection features. Most research combines different attack detection methods in order to get a high accuracy rate in attack detection in addition to NIDS. Put otherwise, a significant amount of overlap exists amongst intrusion detection methods. Table 4 below provides a summary of some research conducted in this area.

An Intrusion Detection and Prevention System (IDPS) based on networks was proposed by Wattanapongsakorn et al. (2012). The

objective of this system is to recognize and react to recognized attack types in a timely and effective manner. The proposed method can be used with different machine learning techniques and assessed in an online network environment. The results show that the proposed IDPS can automatically block future attacks against the victim's computer network and can distinguish between attacks and normal operations with speed and accuracy.

In addition, a proposed methodology was applied in conjunction with the C4.5 Decision Tree algorithm to determine unknown attack types. This algorithm shows effectiveness against unidentified types of network attacks. Nevertheless, by refining the methodology for both the identification of known and new threats, this study can be further enhanced.

Amaral et al. (2014) suggested a network-based intrusion detection system for IPv6-enabled wireless sensor networks. The proposed approach detects assaults using traffic characteristics and unusual activities. Finger2IPv6 and Sniffer are the two components that make up the suggested solution. Network nodes identified as observers are located by the suggested system's intrusion detection system. This makes it possible to watch how neighbors exchange packets and identify possible attack attempts. The rules that NIDS has created are compared to the messages that are seen. If a match is discovered, an alert is generated and sent to the event management system. This proposed approach, as opposed to pre-planned attacks, can detect possible misbehaviors. However, in order to make the system better, new detection rules must be included.

Kumar et al. (2016) designed and evaluated machine learning-based network-based intrusion detection systems to detect network threats. This study builds a variety of supervised machine learning classifiers using datasets and labeled samples of network traffic features generated by different malicious and benign applications. This study's main focus is malware for Android smartphones because of the proliferation of mobile malware and its appeal to users. To test the proposed approach, traffic was generated. Numerous malware samples, such as ransomware, spammers, backdoors, Premium SMS senders, bots, ransomware, information theft, and false antivirus software, were responsible for this traffic. The obtained results demonstrated that the proposed approach could reliably detect known as well as unknown attacks with 99.4% accuracy. This work can be improved by growing the generated dataset and integrating it with the previously mentioned intrusion detection systems.

Qassim et al. (2016) state that an anomaly-based intrusion detection system (AIDS) can identify network traffic that is deemed to be hostile. It sounds an alarm each time it detects an activity that deviates from the usual routines. Handling IDS alarms and distinguishing real warnings from false positives so becomes quite challenging. This study suggested a two-step procedure. In order to find anomalies in the network, they first suggested a set of features for network traffic that are believed to be the most relevant. Second,

it was suggested to use an AIDS alarm classifier to automatically identify behaviors through an anomaly detection system based on packet headers. The authors claim that the recommended method, which is based on machine learning techniques, is successful and efficient in categorizing hostile acts. To enhance this research and increase the accuracy rate, a number of machine learning techniques could be applied.

We describe a brand-new hybrid network-based intrusion detection system (IDS) method that makes use of the AdaBoost and artificial bee colony (ABC) algorithms by Mazini et al. in 2019. The features were selected using the ABC algorithm. The AdaBoost method was used to evaluate and classify the selected characteristics. The NSL-KDD and ISCXIDS2012 datasets were utilized with the recommended strategy in order to evaluate the method's accuracy. A 98.9% accuracy rate is achieved. The authors report that the recommended approach outperformed other IDSs on the same dataset. In later studies, accuracy can be further improved and performance evaluated on other datasets.

Meftah et al. (2019) employed an anomaly-based approach for network intrusion detection using the UNSW-NB15 dataset. Their approach consists of two main steps. Among other techniques, they use Recursive Feature Elimination and Random Forests to select important characteristics for machine learning. Next, in order to find anomalous traffic, they perform a binary classification using a range of data mining algorithms, such as Support Vector Machine, Gradient Boost Machine, and Logistic Regression. They achieved the highest accuracy of 82.11% by using the Support Vector Machine. They then input the SVM's output into a succession of polynomial classifiers to increase the accuracy of identifying various assault types. They evaluated the performance of trees, Decision SVM polynomials, and Naive Bayes in particular. By using the two-stage hybrid classification, the findings' accuracy was increased to 86.04%. This work can be extended on several datasets by applying deep learning techniques or developing a new categorization system. 2020 Devan and Associates.

NIDSs wrongly forecast small groups of attacks due to unreliable data, which results in unreported or incorrectly classified intrusions. Previous studies have addressed the problem of class imbalance by using data-level techniques that increase or decrease the number of occurrences of the minority class. Although these balancing strategies unintentionally improve the performance of NIDSs, they do not address the underlying source of the problem. A two-layer Improved Siam-IDS (I-SiamIDS) strategy was put forth in the Bedi et al. 2021 study in order to address the issue of class imbalance. Both the majority and minority classes are defined by I-SiamIDS as algorithms that do not employ any data level balancing strategies. In order to filter input data, the first layer of I-SiamIDS employs a binary ensemble of Siamese neural networks, eXtreme Gradient Boosting, and Deep neural networks (DNNs). Subsequently, these attacks are routed to the second layer, where the multi-class eXtreme Gradient Boosting classifier (m-XGBoost) is used to classify them

into distinct attack classes. I-SiamIDS shown a significant improvement in recall, accuracy, F1 score, precision, and AUC values for both the CIDDS-001 and NSL-KDD datasets when compared to similar studies. To enhance the clarity of the results, the computational cost analysis of the suggested method is provided as well. Simultaneously, this research can be enhanced by analyzing the outcomes on distinct databases.

IV) Evaluation Of Network-Based IDS

It is well known that network-based intrusion detection systems frequently produce false positives and negatives. Known basic attacks were detected using signature-based detection in the majority of the first network-based intrusion detection systems. Combining several detection techniques has allowed novel devices to attain high accuracy and identify a wider range of assaults. As a result, there are less false positive and negative rates. Another issue is that, in order to account for the features of the observed environment, they frequently need a great deal of tweaking and customization.

While having wide detection, network-based intrusion detection systems have some significant limitations. Among these, managing large traffic loads, processing encrypted communication, and thwarting assaults against IDSs are the most crucial. NIDSs are unable to complete an analysis in the event of a heavy load and are unable to identify assaults on encrypted network traffic. Furthermore, IDS sensors have the potential to miss a number of events, especially when stateful protocol analysis is applied.

A. HOST-BASED IDSs

To identify possible threats, host-based intrusion detection systems, or HIDS, monitor a host's attributes and actions. A host-based IDS keeps an eye on data like traffic statistics, system logs, file access and change, and more. Deshpande et al. (2018) and Gupta et al. (2012)

Agents, or detecting software, are deployed on interest hosts by the majority of HIDS. Every agent keeps an eye on everything within a single host. Data is forwarded by agents to database-server-capable management servers. Monitoring and management are done via consoles. Rather than installing the agent software on each host, some host-based intrusion detection systems (IDSs) make use of specialized hardware. Every device is positioned to keep an eye on traffic on a specific host.

These gadgets are essentially network-based intrusion detection systems (IDSs). Every gadget is made especially to safeguard one of the following:

Server: In addition to observing the server's operating system, the agent can monitor some applications.

Client Host: Agents created to keep an eye on users' hosts frequently examine the operating system and popular programs like web browsers and email clients.

Application Service: Some agents, like web servers or database servers, are made exclusively to watch over a particular application. We also refer to these agents as application-based IDSs.

TABLE 4. Summary of Host-Based Intrusion Detection Methods.

Paper/Year	Proposed Method	Goals/Success
Kumar and Sangwan 2012	Signature-based attack detection was performed using Snort.	This IDS System can detect and analyze intrusions in real-time network traffic. This study will help new users to understand the concept of Snort-based IDS.
Uddin et al.2013	A proposed new Signature-Based Multi-Layer IDS model using mobile agents.	The proposed model is able to detect threats with a high success rate. It also provides a mechanism to periodically, update these small signature databases.
Hubbali and Suryanarayanan 2014	Possible techniques for minimizing false alarm rate in signature-based Network Intrusion Detection System (NIDS) are examined.	Despite all known techniques, there are still problems that need to be addressed. This study can help security researchers to implement a new post processing technique for IDS alerts.
Rai et al.2016	A decision tree algorithm based on the C4.5 decision tree approach.	The proposed Decision Tree Splitting (DTS) algorithm is an effective method for signature-based attack detection.
Aldwairi e al. 2017	A vector algorithm is parallelized on a multi-core CPU under the MapReduce framework.	Phoenix++ and MAPCG MapReduce applications showed 1.3 and 1.7 times improvement over MPI, respectively.
Baykara and Das 2018	A honeypot based approach for intrusion detection/ prevention systems is proposed. The developed application is combined with IDSs to analyze data in real-time and to operate effectively.	The developed system is able to show the network traffic on servers visually in real-time animation. It can detect zero-day attacks. This system also helps in reducing the false positive level in IDSs.
Baykara and Das 2019	A centralized honeypot-based approach with a software-defined switching is proposed.	The proposed system has been run in GNS3 simulation software and good results have been obtained by reducing false alarm level, network traffic, and cybersecurity cost.
Gunduz and Das 2021	The objectives, requirements, threats and potential solutions of the IoT-based smart grid are analyzed.	The paper presents specific solutions to threats on IoT-based smart grid applications and highlights possible research opportunities for researchers to provide future research directions.
Malek et al., (2022)	A new system detect intrusions using a set of rules as a pattern recognized engine.	The combination of experimental results, SBID and PBID approaches provides a comprehensive system for intrusion detection.
Otoum and Nayak 2023	An intrusion detection model called AS-IDS.	An attack detection rate of 96.9% was achieved on the NSL-KDD dataset.
Zahedi et al. 2023	DL algorithms, such as deep reinforcement learning and Hidden Markov Models, still require further attention	Detecting hidden attacks is the main obstacle for both SIDS and AIDS

Fig 2: Host-Based Intrusion

Detection Methods (Malek et al., 2022)

Q2. What are the Intrusion Detection Technologies?

Intrusion detection methodologies mainly divided into threedistinct categories including:

a. Signature-based model;
b. Anomaly-based model;
c. Stateful protocol analysis;

Different techniques are used by different IDS methodologies to detect network attacks. Signature-based detection is very quick and efficient for known attack types, but it is not able to identify zero-day assaults. Although anomaly-based approach produces false alarms, it is effective in detecting previously undiscovered network-based threats. Stated differently, it considers regular traffic to be an attack. Although stateful protocol approach is resource-intensive, complex, and unable to identify smart attacks, it can detect some new types of attacks. Each methodology's specifics are listed below.

A. Signature-Based Model

A pattern that correlates to a known assault is called a signature. The practice of correlating signatures with observable events in order to identify possible attacks is known as signature-based detection. Farshchi (2003). Should a match occur throughout the comparison process, the system will provide an additional report or a warning. Examples of signatures include: an attempt at an attack using the login "root," endangering the network's security; an email titled "Free programs," which is indicative of well-known and widespread malware; or an operating system stating in the system log that host control is disabled.The simplest detection technique is signature-based detection, which compares observed events via a comparison procedure to a collection of signatures. A warning is provided if the list contains an attack condition that has already been defined. While signature-based intrusion detection systems (IDSs) are highly efficient in identifying known threats, they are not very good at identifying unexpected threats or variations of known threats. For instance, a signature searching for the malicious file "prog.exe" would not match if the attacker replaced it with the name "prog2exe." Farshchi. (2003).

1) Related Work

Table 5 summarizes signature-based IDS approaches and looks at

each study's performance as well as the basic principle of the suggested strategy. Snort was used in the study by Kumar and Sangwan (2012) to detect attacks based on signatures. The DARPA Dataset was sent over the network and examined anomalous linkages found during transmission in order to conduct intrusion detection using Snort. A well-known NIDS for examining network packets and matching them to a database of recognized attack signatures is called Snort. Furthermore, the Snorts attack signature database may be updated from time to time. The ability to identify and evaluate intrusions in real-time network traffic has been shown by this IDS system. The authors claim that this study will aid in the comprehension of Snort-based IDS by novice users. Additionally, this study might be enhanced by using and evaluating various intrusion detection technologies. Dealing with massive amounts of incoming traffic when each packet needs to be cross-referenced with every signature in the database is a significant problem for signature-based intrusion detection systems. An intrusion detection system suppresses packets in order to miss possible attacks when it is unable to handle the volume of traffic. In 2013, Uddin et al. proposed.

TABLE 5: Summary of Signature Based Intrusion Detection Prevention Methods.

Paper/Year	Proposed Method	Goals/Success
Kumar & Sangwan 2012	Signature-based attack detection was performed using Snort.	This IDS System can detect and analyze intrusions in real-time network traffic. This study will help new users to understand the concept of Snort-based IDS.
Uddin et al. 2013	A proposed new Signature-Based Multi-Layer IDS model using mobile agents.	The proposed model is able to detect threats with a high success rate. It also provides a mechanism to periodically, update these small signature databases.
Hubbali & Suryanarayanan 2014	Possible techniques for minimizing false alarm rate in signature-based Network Intrusion Detection System (NIDS) are examined.	Despite all known techniques, there are still problems that need to be addressed. This study can help security researchers to implement a new post processing technique for IDS alerts.
Rai et al. 2016	A decision tree algorithm based on the C4.5 decision tree approach.	The proposed Decision Tree Splitting (DTS) algorithm is an effective method for signature-based attack detection.
Aldwairi e al. 2017	A vector algorithm is parallelized on a multi-core CPU under the MapReduce framework.	Phoenix++ and MAPCG MapReduce applications showed 1.3 and 1.7 times improvement over MPI, respectively.
Baykara and Das 2018	A honeypot based approach for intrusion detection/prevention systems is proposed. The developed application is combined with IDSs to analyze data in real-time and to operate effectively.	The developed system is able to show the network traffic on servers visually in real-time animation. It can detect zero-day attacks. This system also helps in reducing the false positive level in IDSs.
Baykara and Das 2019	A centralized honeypot-based approach with a software-defined switching is proposed.	The proposed system has been run in GNS3 simulation software and good results have been obtained by reducing false alarm level, network traffic, and cybersecurity cost.
Gunduz and	The objectives,	The paper presents specific solutions to threats on

Das 2020	requirements, threats and potential solutions of the IoT-based smart grid are analyzed.	IoT-based smart grid applications and highlights possible research opportunities for researchers to provide future research directions.
Malek et al. 2020	A new system detect intrusions using a set of rules as a pattern recognized engine.	The combination of experimental results, SBID and PBID approaches provides a comprehensive system for intrusion detection.
Otoum & Nayak 2021	An intrusion detection model called AS-IDS.	An attack detection rate of 96.9% was achieved on the NSL-KDD dataset.
Rovito et al. 2022	Used genetic algorithms and genetic programming method	Implemented two classification models for the identification of bot accounts on the Twitter platform
Safana et al. 2023	System detect intrusions using a set of rules as a pattern recognition	IDS are used to monitor networks and send alerts when suspicious activity on a system or network is detected while an IPS reacts to cyberattacks in real-time with the goal of preventing them
Hami et al. 2024	Hybrid method was proposed to overcome feature selection and imbalanced data challenges in IDPSs, The method, called Convolution neural network and deep watershed auto-encoder (CNN-DWA)	The analysis indicates that these methods generally detected attacks with high ACC rates

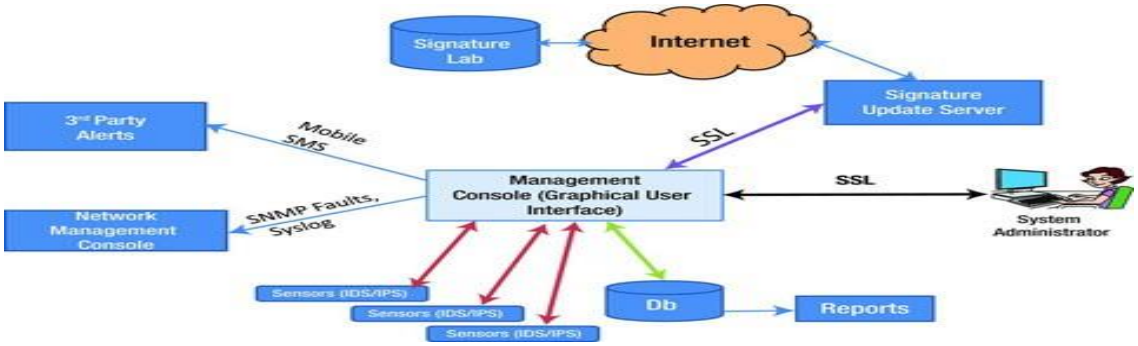

Fig 3: Signature Based Intrusion Detection Prevention (Uddin et al. 2013)

As seen in Table 4 above, a novel Signature-Based Multi-Layer Intrusion Detection System (IDS) model that makes use of mobile agents may identify threats with a high success rate by automatically and dynamically generating and utilizing numerous small and large databases. Additionally, it offers a way to use mobile agents to update these tiny signature databases on a regular basis. An automated system that can transfer, add, and remove signatures between databases of various IDS systems can be created using the suggested approach.

Potential methods for reducing the false alarm rate in signature-based Network Intrusion Detection Systems (NIDS) are investigated by Hubbali and Suryanarayanan (2014). In signature-based intrusion detection systems, false alarm minimizing strategies are categorized along with their benefits and drawbacks. A review is also conducted on the

effectiveness of a number of the top Security Information and Event Management tools that apply these methods. The authors claim that issues still need to be resolved in spite of all existing methods. Security researchers can use this study's findings to put new post-processing methods for IDS alarms into practice. Subsequent investigations ought to tackle distinct research concerns that will augment the practicability of the suggested methodologies.

For Rai et al.'s 2016 study, a decision tree method built on the C4.5 decision tree technique was developed. Feature selection and split value are important considerations when building a decision tree. This work's developed method aims to address these two issues. What matters are the values that, when choosing the split value and the information gain when choosing the features, will make the classifier unbiased against the most common values. The NSL-KDD dataset was utilized to evaluate the proposed approach, and the experiment was conducted in accordance with the number of features. The time required to build the model and the degree of accuracy reached were among the metrics. The authors claim that a successful method for detecting signature-based attacks is the Decision Tree Splitting (DTS) algorithm. This study can be made better by increasing the split value and decreasing the number of features used. Aldwairi et al. 2017 aim to speed up the method and reduce the matching load of the signature-based model by parallelizing the signature matching process on a multi-core CPU. This study parallelizes the vector technique Myers on a multi-core CPU using the MapReduce framework. The multi-core program achieves acceleration around four times faster than the serial version. They also parallelized the Myers technique using two different MapReduce implementations. The suggested approach's implementation is contrasted with an earlier algorithmic implementation that relied on a message passing interface (MPI). Based on the findings Applications such as Phoenix and MAPCG Map Reduce shown improvements over MPI of 1.3 and 1.7 times, respectively. Gunduz and Das 2020 proposed a novel approach to intrusion detection that uses a set of rules as a pattern recognition engine. In order to verify previous uses of a Pattern Based Intrusion Detection (PBID) model, they utilized a Statistical Based Intrusion Detection (SBID) model. The proposed model was tested using the dataset that was created during the course of the inquiry. A 75% accuracy rate has been achievedThe combination of experimental results and PBID and SBID approaches provides a comprehensive approach to intrusion detection, according to the authors. Nevertheless, relying solely on signature-based attack detection will not result in an effective detection. Therefore, by including anomaly-based intrusion detection, this work can be further refined.

Malek et al. 2020 introduce an intrusion detection model called AS-IDS that combines these two techniques to detect known and new attacks in Internet of Things networks. The proposed model consists of three stages: traffic filtering, hybrid IDS, and preprocessing. At the IoT gateway, network traffic is first filtered according to packet characteristics that match. The Target Encoder, Z-score, and Discrete Hessian Eigenmap (DHE) are then applied in the preprocessing stage, in that order. In the last stage, the signature basis and the anomaly-based model are combined. In the part on the signature-based system, the Generalized Suffix Tree (GST) technique is applied to compare signatures and classify attacks as either intruder, normal, or unknown. The anomaly-based system use Deep Q-learning to recognize unknown attacks and classifies assaults using bandwidth and Signal to Noise Ratio (SNR). The proposed AS-IDS model has been built and tested in real-time traffic using the NSL-KDD dataset. A rate of 96.9% assault detection was achieved. This study can be used to obtain extensive experimental results on various datasets.

2) Evaluation of Signature-Based Model

The easiest and most understandable detection technique is signature-based detection. Activities like packets and log entries are compared by the system with a list of registered signatures. Users can thus manage the signature database, and the system administrator can quickly determine the kinds of attacks that will raise red flags. While signature-based intrusion detection systems (IDSs) are highly successful in identifying known attacks, they are not very good in identifying undiscovered threats, lurking dangers, or any variation of existing threats. A distinct signature needs to be defined for each attack type that an attacker can launch in order to have a high success rate, and the signature database needs to be updated.

B. Anomaly-Based Model

The practice of identifying anomalous occurrences by contrasting observed behaviors with notions of normalcy is known as anomaly-based detection Otoum and associates, (2021). Rules in an anomaly-based detection system (AIDS) reflect typical user, host, network connection, or application behavior. These guidelines were created throughout time by paying attention to the traits of typical behavior. For instance, the average amount of time spent on the internet during business hours is the rule for a network. The IDPS then compares the features of the current activity with the criteria, using statistical techniques to identify web activity that is much more than anticipated and to create alerts. Several behavioral characteristics, such the quantity of emails a user sends, the number of unsuccessful login attempts, and the quantity of packets exchanged in a specific amount of time, can all have rules created for them. The main benefit of anomaly-based detection techniques is

their ability to identify attack types that were previously unidentified. Let's say, for example, that a machine has a fresh kind of virus on it. The malware has the ability to use up all of the computer's processing power, send a lot of emails, establish a lot of network connections, and carry out other actions that can be very different from the profiles that were made for the machine.

There are two kinds of rules designed for anomaly-based detection: static and dynamic. Unless the IDPS is instructed to produce a new rule, the static rule list remains unchanged once it is created. As new events are noticed, a dynamic list is updated continuously. Measures of normal behavior adapt to the systems and networks they are a part of. A static list needs to be updated on a regular basis because it eventually expires. Although dynamic profiles don't have this issue, attackers may try to hijack them. An attacker might, for instance, start off with a modest volume of harmful activity before gradually increasing both the frequency and volume of activity. IDPS may include harmful activity in its profile and view it as typical behavior if the pace of change is slow enough. An frequent issue with anomaly-based IDPS products is the unintentional inclusion of harmful actions as part of the rule.

An additional issue with anomaly-based IDPSs is that it can occasionally be challenging to implement the rules correctly. For example, if a huge file transfer event happens just once a month, this behavior is not routinely seen, which makes it potentially odd and may cause an alert to go off. Particularly in unfamiliar or dynamic contexts, benign activity that departs greatly from the rules frequently results in a large number of false positives for anomaly-based intrusion detection systems. The inability to identify the source of the alert or confirm that it is not a false positive is another significant issue with the application of anomalous-based detection approaches, which arises from the volume and complexity of occurrences

1) Related work

Table 5 provides a summary of the literature review on anomaly based detection techniques. Each paper's fundamental thesis as well as the benefits and drawbacks of each study have been outlined. An anomaly-based intrusion detection system was presented by Samrin and Vasumathi in 2017 as a way to boost productivity and decrease false alarms. Modeling with fuzzy rules.

Table 5: Summary of Anomaly-Based Intrusion Detection Prevention Methods.

Paper/Year	Proposed Method	Goals/Success
Geramiraz et al.2012	An anomaly-based intrusion detection system.	Test results significantly improved he performance of the system by about 20% using adaptive IDS. The proposed anomaly-based

		intrusion detection improved the accuracy of the system by around 15%.
Yassin et al. 2013	Integrated machine learning algorithm based on K-means clustering and the Naiv Bayes Classifier (NBC) named KMC+NBC.	Performance evaluations were made on the ISCX-2012 dataset. KMC+NBC increased the accuracy and detection rate up to 99% and 98.8%, respectively, while reducing the false alarm to 2.2%.
Narsingyani & Kale 2015	Genetic algorithm (GA) based anomaly detection technique.	KDD99cup dataset was used and according to the results False Positive alarm rate can be reduced and detection speed can be increased.
Harish & Kumar 2017	An anomaly-based method based on fuzzy clustering.	EDA dataset, which is a variant of the KDD dataset, was used. 86.3% accuracy and 17.04% false alarm rate were obtained.
Aljawarneh et al. 2018	A new hybrid model.	An accuracy rate of 99.81% and 98.56% was obtained for the dual-class and multi-class NSL-KDD datasets, respectively.
Tama et al. 2019	A method for selection of relevant features and an intrusion detection system based on two-level ensembles of classifiers.	An accuracy rate of 85.8% in the NSL-KDD dataset and 91.3% in the UNSW-NB15 data was achieved.
Viegas et al. 2019	An IDS approach capable of processing evolving network traffic while being scalable to large packet rates is called BigFlow.	Experiments were made over a network traffic dataset spanning a full year, BigFlow can maintain high accuracy over time. It requires as little as 4% of storage and between 0.05% and 4% of training time, compared with other approaches.
Dwivedi et al. 2020	A new technique by combining Ensembles of Features Selection and Adaptive Grasshopper Optimization Algorithm methods, called as EFSAGOA.	EFSAGOA has been evaluated on intrusion data as ISCX 2012. It has provided a high detection rate of 99.23%, accuracy of 99.13% and a low false alarm rate of 0.067.
Eskandari et al. 2020	An anomaly-based intelligent intrusion system named Passban.	Passban can detect attacks with low false positive and high accuracy rates.
Kumar et	An anomaly-	Proposed model is tested using an

al.2021	based intrusion detection system by decentralizing the existing cloud based security architecture to local fog nodes.	actual IoT-based dataset. The evaluation of the underlying approach outperforms in high detection accuracy and low false alarm rate using Random Forest algorithm.

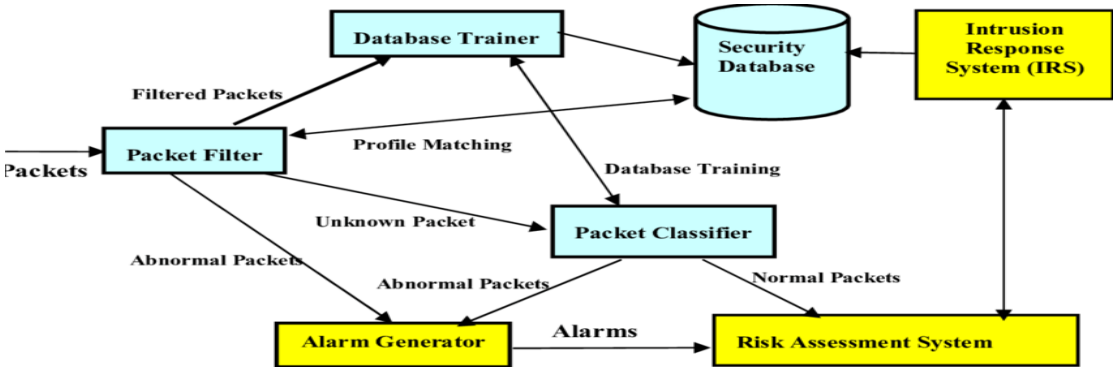

Fig 4: Anomaly-Based Intrusion Detection Prevention (Malek et al., (2022)

A new security mechanism against distributed denial-of-service (DDoS) flood attacks is shown in Figure 4 above, shielding network servers, network routers, and client hosts from becoming handlers, zombies, and victims. USC created the Net Shield system to defend any public IP network over the Internet.

During the development and testing stages, the model was updated using fuzzy controllers, respectively. Furthermore, the system user is presented with the outcomes of the system estimations. Following the system user's validation of the judgments, the fuzzy controller modifies the detection model based on input from the system user. The system was evaluated using the NCL dataset. A portion of the KDD '99 dataset makes up this dataset. The authors claim that by employing adaptive IDS, their test results considerably increased the system's performance by roughly 20%. Additionally, the system's accuracy was increased by about 15% thanks to the suggested anomaly-based intrusion detection method. It is also possible to test this suggested intrusion detection system using various datasets.

In order to maximize detection and accuracy while avoiding false alarms, Geramiraz et al. (2012) present an integrated machine learning technique called KMC NBC, which is based on K-Means clustering and the Naive Bayes Classifier (NBC). The labeling procedure has been implemented using K-Means clustering. Using K-Means, all the data are gathered into the appropriate clusters based on their behavior, which may be classed as aggressive or normal. The misclassified data are then reclassified using the Naive Bayes Classifier.

KMC+NBC and NBC's performances were assessed using the ISCX-2012 dataset. The findings show that KMC NBC decreased the false alarm to 2.2% while increasing accuracy and detection rate to 99% and 98.8%, respectively. Methods for feature selection could be added to this investigation..

One of the most successful evolutionary strategies in machine learning, genetic algorithm (GA) based anomaly detection technique was used by Yassin et al. (2013) to detect network attacks. The optimization of the false positive rate was the primary focus of this study because it is expected that a drop in this rate would also boost accuracy and performance. This study discusses the limitations of alternative accuracy techniques for their false positive rate. The trials were conducted using the KDD99cup dataset. The results show that by choosing features carefully, the False Positive alert rate may be decreased and detection speed can be raised. The identification of more significant features for this work can be enhanced by applying dynamic feature selection approaches

A fuzzy clustering-based anomaly-based approach for identifying network anomalies was introduced by Narsingyani and Kale in 2017. Three steps make up the suggested method: preprocessing, feature selection, and clustering. Duplicate data were removed from the dataset during preparation. Then, the distinctive traits were chosen using principal component analysis. During the clustering phase, the Robust Spatial Kernel Fuzzy C-Means (RSKFCM) technique was employed to group the network samples. RSKFCM is a variant of the conventional Fuzzy C-Means algorithm that employs the kernel distance metric and considers neighborhood data. The EDA dataset, a variation of the KDD dataset, was utilized to assess the suggested method in comparison to the industry standard methods. Performance metrics included accuracy, false positive rate, and cluster validity indices. Results showed an accuracy of 86.3% and a false alert rate of 17.04%. The authors claim that the suggested approach produced superior outcomes over alternative approaches. Nonetheless, this research can be enhanced by employing distinct techniques like the Evolutionary algorithm.

In 2017, Harish and Kumar created a new hybrid approach to estimate the intrusion coverage threshold based on the best features of network transaction data. The 20% test dataset and the NSL-KDD dataset—a binary and multi-class problem—were utilized in the evaluation of the suggested model. The results show that for estimating the feature association impact scale, the hybrid technique significantly reduces the computation and time cost. The dual-class and multi-class NSL-KDD datasets yielded accuracy rates of 99.81% and 98.56%, respectively. In addition, there are issues with both low and high false negative rates. To tackle these issues, a hybrid strategy comprising of two primary components has been suggested. First, key elements that will improve the suggested model's

accuracy are chosen using the Information Gain and Vote approach, which mixes probability distributions. The hybrid algorithm then employed the AdaBoostM1, REPTree, J48, Random Tree, Naïve Bayes, Meta Pagging, and Decision Stump classification techniques. Improved accuracy, a high rate of false negatives, and a low percentage of false positives were the outcomes. This research can be advanced by utilizing the suggested approach on various datasets using various optimization strategies.

A technique for choosing pertinent features and an intrusion detection system built on two-level ensembles of classifiers are presented in the work by Aljawarneh et al. (2018). Three distinct techniques were employed to decrease the training datasets' feature sizes: genetic algorithms, ant colony algorithms, and particle swarm optimization. A reduced error pruning tree (REPT) is used to choose features depending on classification performance. Then, two-level classifiers called rotation forest and bagging algorithms are used. The UNSW-NB15 and NSL-KDD datasets were utilized to assess the suggested system. An NSL accuracy percentage of 85.8%The authors report that their results greatly outperformed other recently published classification algorithms, with 91.3% in the UNSW-NB15 dataset and -KDD dataset. New methods that use fewer features to attain higher accuracy can be used to further develop this work.

Dwivedi et al 2020. propose Passban, an anomaly-based intelligent intrusion detection system (IDS) that can guard directly linked Internet of Things (IoT) devices. One of the suggested system's features is that it may be directly installed on inexpensive IoT gateways This capability allows it to fully leverage the edge computing paradigm for cyber threat detection as close to the data sources as feasible. During the Passban evaluation stage, two distinct scenarios were used. In the first case, Passban was employed as an IDS that operated directly on the gateway that was receiving data from the Internet and Internet-connected devices. In the second case, the infrastructure element is a "security in the box," which is a unique gadget that accepts traffic from the local gateway and the Internet. The evaluation findings show that Passban can identify attacks like HTTP and SSH Brute Force, Port Scanning, and SYN Flood with minimal false positive and high accuracy rates.

2) Evaluation Of Anomaly-Based Model

Anomaly-based detection is based on the principle of comparing traffic with what is considered normal to identify different situations. Anomaly-based intrusion detection systems are considered a better option than signature-based systems, as they do not require prior knowledge of the attack signature to detect an attack. But at the same time, the alarms generated by this system are more difficult to manage than signature-based intrusion detection systems. This may be because signature-based IDS generates information along with reported alarms, while anomaly-based IDS identifies traffic flow that is detected as

malicious.

It is therefore crucial to identify the classes of a detected attack even though anomaly-based detection systems are capable of detecting unknown attacks. An anomaly-based intrusion detection system (IDS) raises an alarm whenever it observes an activity that deviates from the fundamental pattern of normal behavior, but it is not aware of the cause of the anomaly, which poses a significant challenge to managing alarms and differentiating between false positives and true alarms.

C. Stateful Protocol Analysis

In stateful protocol analysis, deviations are found by comparing actual events with preset profiles of widely accepted normal protocol activities for each protocol state. While stateful protocol is based on universal profiles that define how protocols should or shouldn't be utilized, anomaly-based detection uses host-based or network-based profiles.The term "stateful" in stateful protocol analysis refers to an intrusion detection system's (IDS) capacity to comprehend and track the state of the network, transport, and application protocols. For instance, an FTP (File Transfer Protocol) session is first started by the user without authentication. In this instance, the commands that unauthenticated users can execute are limited to displaying help information and entering their login and password

TABLE 6. Summary of Stateful Protocol Analysis

Paper/Year	Proposed Method	Goals/Success
Mudzingwa and Agrawal 2012	A detailed review of main techniques used in intrusion detection and prevention systems.	Anomaly-based technique is superior to other techniques, but most of the IDPS use a combination of the main methodologies.
Seo et al. 2013	A stateful SIP inspection mechanism called SIPAD.	The proposed approach significantly reduces the operating cost. It can be used even in resource-constrained environments such as smartphones.
Yang et al.2014	A stateful Intrusion Detection System that uses the Deep Packet Inspection method.	A proposed approach specifically designed for the IEC 60870-5-104 protocol. The new intrusion detection approach has been tested and validated.
Kang et al. 2016	A framework for detecting smart grid attacks.	The attacks that can create dangerous situations can be detected effectively.
Boite et al.2017	The stateful paradigm is named StateSec.	StateSec detects and mitigates various attacks such as DDoS and port scans with high accuracy.
Lewis et al. 2019	A filtering approach named as P4ID.	This system was evaluated by combining the CICS2017 dataset and the Emerging Threats rule set. A significant reduction in traffic handled by IDS can be achieved.
Sharma et al.2019	A lightweight behavior rule specification-based misbehavior detection for the IoT-embedded cyber-physical systems (BRIoT).	The proposed approach is verified by an embedded system in an embedded system in an unmanned aerial vehicle. The feasibility of the proposed model is demonstrated with high reliability, low

		operational cost, low false-positives, low false-negatives, and high true positives in comparison with existing rule-based solutions.
Rashid et al.2020	A comprehensive and comparative analysis of the NSL-KDD and CIDDS-001 datasets.	KNN, SVM, NN and DNN classifiers have approximately 99% accuracy in the k-NN and Naïve Bayes classifiers CIDDS-001 dataset.
Sbai and Elboukhari 2020	An IDS using deep neural network technology to detect the subclass of the big class DDoS: Data flooding attack.	The proposed model evaluated on the dataset CICDDoS2019. The obtained results show that the proposed architecture model achieves interesting performance (Accuracy, Precision, Recall and FI-score).
Choudharry and Kesswani 2021	A hybrid classification approach to detect multi-class attacks in the IoT network.	The 81.02% detection rate, 2.22% false alarm rate and 92.85% detection rate, 2.99% false alarm rate were obtained respectively on UNSW-NBI5 and NSL-KDD dataset.

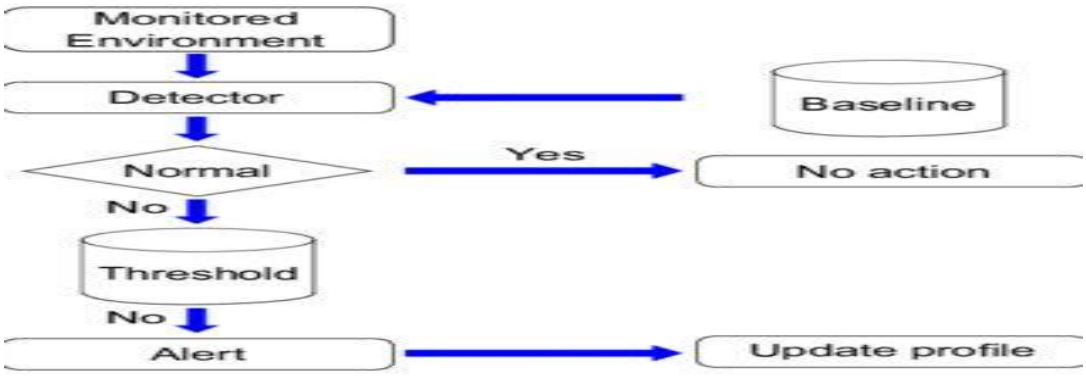

Fig 5: Stateful Protocol Analysis (Kang et al. 2016)

As seen in figure 5 above, the World Wide Web has developed into a robust, adaptable, and sizable platform for the delivery of applications and the spread of information. It began as a system for providing an interconnected collection of static pages. Sensitive information and vital resources are being posted online by businesses and organizations more frequently. Regrettably, the rapid rise in popularity and power of the internet has also led to a rise in the quantity and severity of cybercriminals. Because of how serious the issue is, there is a lot of interest in the security sector to find ways to lessen the threat. In order to do this, intrusion detection and prevention systems, or IDPSs, have been suggested as a possible tool for spotting and stopping computer network exploits that are effective. This document provides a thorough description of each existing intrusion and prevention systems methodology along with an overview of them. Furthermore, we present a comparative analysis of different approaches to facilitate an intuitive understanding of IDPS as a whole.

Q3. What is the Conceptual

research studies conducted in the field of IDPSs?

Intrusion Prevention Systems (IPSs) are now commonly acknowledged as a potent instrument and a crucial component of IT security measures. Any device that can identify and stop known as well as unknown assaults is an intrusion prevention system (IPS). There is one feature that sets IPS technology apart from IDS technologies. When an intrusion is discovered, intrusion prevention systems (IPS) might react by trying to stop it from happening. They can be categorized into the following groups based on the various reaction mechanisms they employ..

A) Response Techniques of IPS

IPS thwarts the actual attack. It can stop access to the target from the offending user account, IP address, or other attacker attribute. It can also terminate the network connection or user session that is being utilized for the attack. An IPS can alter the security landscape. To stop an attack, the IPS could alter how other security measures are configured. The attack's content is modified by the IPS. IPS systems have the ability to neutralize an attack by removing or replacing its destructive elements.

B) Approaches to Intrusion Prevention Systems

There are different types of approaches is used in the IPS to secure the network.

i). Signature-Based IPS: It's frequently employed by numerous IPS systems. Devices that recognize a pattern that the majority of attacks exhibit are given signatures. For this reason, pattern matching is another name for it. To counter new attacks, these signatures can be added, adjusted, and updated.

ii). Anomaly-Based IPS: Another name for it is profile-based. It looks for activity that deviates from what an engineer considers to be typical behavior. Statistical and non-statistical anomaly detection are two types of anomaly-based approaches. Policy-Oriented IPS: It is primarily focused on upholding the organization's security policy. When actions are found that go against the organization's security policy, alarms are set off. This kind of technique incorporates security policy directly into the IPS device..

iii).**Protocol-Analysis-Based IPS:** is comparable to the signature-based method. The protocol analysis-based approach is more versatile in identifying certain sorts of attacks and can perform much deeper packet inspection than most signatures, which only look at common settings. Nalavade2011 and associates.

Table 7: General Evaluation of IDPS

Author/Year	Methodology/ Tools	Contribution	Research Gap

(Rovito et al. 2022b)	Used genetic algorithms and genetic programming method	implemented two classification models for the identification of bot accounts on the Twitter platform	The 25 per cent undetected bots could pose a great treat to the social media users
(Callejasolanas et al. 2021)	DT, KNN, LR, Naive Bayes and Bag of Words (BOW) model	Computationally effective and higher detection rate of bots compared to other algorithm	Difficult to detect bots that uses other terminologies not captured by BOW in larger dataset
(Kosmajac and Keselj 2019)	Digital fingerprint, Naive Bayes,	Detect twitter bot using user activity fingerprint,	Computational overhead will affect real-time
Adam et al.2020	SVM, LR, KNN, RF, and Gradient Boosting	complemented with a set of well-known statistical diversity measures	implementation
(Wei and Nguyen 2021)	Bidirectional Long Shortterm Memory Neural Networks and Word Embeddings	The model only rely on tweets and does not require heavy feature engineering to detect bots on Twitter	Tweets alone are not reliable to determine the suitability of the classification of Twitter users
(Efthimion, Payne, and Proferes 2018b)	Logistic Regression and Support Vector Machine	Achieved 95.77% accurate, with a misclassification rate of 4.23%	Degradation in performance when exposed to large dataset
(Kudugunt and Ferrara 2018a)	Long Shortterm Memory Neural Networks	Used LSTM architecture that exploits both content and metadata to detect bots	Prone to over fitting and it takes longer time to train
(Azab et al. 2016)	Classification algorithms (RF, SVM, Decision Tree, Naive Bayes, Neural Network	From more than 22 attributes, the model proposed reached only seven effective attributes for fake accounts detection	Detection features were based on fake accounts not bots
(Rahman et al. 2021)	R language and Python machine learning	DT-SVMNB that classifies users as depressed one or suicidal one in the	Focus was on predicting vulnerable users on the social

Conclusion

The cornerstone of technology is made up of IPS and IDS, which track

and monitor network traffic, identify suspicious activity, stop it, and notify the administrator of any necessary steps. Intrusion prevention systems (IPS) and intrusion detection systems (IDS) vary primarily in that IPS is a control system and IDS is a monitoring system. While IPS blocks packets from delivering depending on their contents, much like a firewall blocks traffic based on IP address, IDS won't change network traffic.

An IPS responds to cyberattacks in real time with the aim of preventing them from accessing targeted systems and networks, whereas IDS monitors networks and sends alerts when suspicious activity on a system or network is discovered.Attacks related to cyberspace are growing rapidly, and there is currently no proven way to halt them all. IDPS is among the most crucial methods for reducing or eliminating cyberattacks. Furthermore, in order to get beyond IDSs, firewalls, and antivirus programs, attackers are utilizing the newest techniques and technology. One may argue that a well-executed zero-day attack won't be detected by the computer-based system.

The weak spots of the current IDSs must be fixed, and current IDSs must be merged with new technologies like cloud, machine learning, and deep learning in order to boost the detection of new and complex cyber-attacks. An overview of the earliest intrusion detection systems is given in this document, along with information on the methods used, different approaches to detection, and the main idea behind each detection methodology. Subsequently, an analysis is conducted on the existing state-of-the-art research, available datasets, and the benefits and drawbacks of every detection system. Lastly, a comparison of detection methods, potential research directions, and our opinions of IDSs are provided.

Network-based intrusion detection systems are useful for spotting network intrusions. Both the detection rate and the variety of attacks are increased by the integration of different detection techniques. NIDSs have trouble identifying attacks on network traffic that is encrypted. Conversely, host-based intrusion detection systems identify host attacks. Host-based intrusion detection systems often employ many detection methods to boost the rate of detection. IDSs that are wireless offer excellent detection capabilities. They are unable to identify offline processing assaults and passive monitoring in wireless communications, though. While fast and efficient in identifying known attacks, signature-based detection methods fall short in identifying unknown ones. When an anomaly-based intrusion detection system detects activity that diverges from typical attack patterns, it raises an alarm. While it can identify new attack types, the anomaly-based intrusion detection system also generates false alerts. We came to the conclusion that every detection strategy works better on different datasets and has pros and cons of its own. The size, dimensionality, amount of characteristics available, and distribution of the data are among the features that can be used to assess how well IDS techniques work. It can be claimed that the current IDS makes

sufficient use of statistical, heuristic, and pattern-based techniques. As a result, researchers should concentrate more on deep learning, machine learning, and cloud-based methods. Researchers and developers must be mindful of evasion strategies such address spoofing, avoiding defaults, evading pattern changes, coordinated low-bandwidth attacks, and fragmentation while developing an intrusion detection system (IDS).

The well-known IDS datasets are also examined. Every dataset has advantages and disadvantages of its own, and is more useful in certain contexts. The largest and most popular dataset for IDSs is KDD '99, yet the ML classification process is difficult due to the dataset's numerous duplicated characteristics. The NSL-KDD dataset represents a KDD modification. The NSL-KDD dataset is a good way to evaluate modern IDSs because it doesn't contain any modern network assaults. Different problems can be found in other datasets, including CAIDA, ADFA-LD and ADFA-WD, AWID, UNSW-NB15, and CICIDS. These datasets are widely used in scientific research and are well-liked by network intrusion detection systems. IDS datasets and characteristics must be updated periodically to assess the accuracy of potential future network intrusions because network attacks are constantly changing. The paper also covered the available IDS tools. Different IDS tools can work better for different scenarios and operating systems. This is a result of the dynamic and changing needs of businesses. Other factors that must be considered when selecting the best appropriate IDS for the target system include the bandwidth of the networks, the performance of the IDS, the scalability of the IDS tools, the size of the organization, and the complexity of the victim system.

References

Abdulhammed, M. Faezipour, A. Abuzneid, and A. Alessa, 2018 "Effective features selection and machine learning classifiers for improved wireless intrusion detection," in Proc. Int. Symp. Netw., Comput. Commun. (ISNCC), Jun. 2018, pp. 1–6.

Administrator Guide. Security Event Manager, Version 2021.2. Accessed: Jun. 30, 2021. [Online]. Available: https://documentation solarwinds.com/en/ success_ center/sem/content/ sem_administrator_ guide.htm

Afzal, J. Rossebø, B. Talha, and M. Chowdhury, 2016 "A wireless intrusion detection system for 802.11 networks," in Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET), Mar. 2016, pp. 828–834.

Ahn, H. Yi, Y. Lee, W. R. Ha, G. Kim, and Y. Paek, 2020 "Hawkware: Network intrusion detection based on behavior analysis with ANNs on an IoT device," in Proc. 57th ACM/IEEE Design Autom. Conf. (DAC), Jul. 2020, pp. 1–6.

Aldwairi, A. M. Abu-Dalo, and M. Jarrah, 2017 "Pattern

matching of signature-based IDS using Myers algorithm under MapReduce framework," EURASIP J. Inf. Secur., vol. 2017, no. 1, pp. 1–11, 2017.

Aldwairi, A. M. Abu-Dalo, and M. Jarrah, 2017 "Pattern matching of signature-based IDS using Myers algorithm under mapreduce frame- work," EURASIP J. Inf. Secur., vol. 2017, no. 1, pp. 1–11, Dec. 2017.

Aldweesh, A. Derhab, and A. Z. Emam, 2020 "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowl.-Based Syst., vol. 189, Feb. 2020, Art. no. 105124.

Aleesa A.M., Zaidan B.B, Zaidan A.A, and Sahar N.M 2020, "Review of intrusion detection systems based on deep learning techniques: Coherent taxonomy, challenges, motivations, recommendations, substantial anal- ysis and future directions," Neural Comput. Appl., vol. 32, no. 14, pp. 9827–9858, Jul. 2020.

Aljawarneh, M. Aldwairi, and M. B. Yassein, 2018"Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," J. Comput. Sci., vol. 25, pp. 152–160, Mar. 2018.

Alrajeh .A, N,, Khan S, and Shams B.2013 "Intrusion detection systems in wireless sensor networks: A review," Int. J. Distrib. Sensor Netw., vol. 9, no. 5, May 2013, Art. no. 167575.

Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han, and L. Shu, 2016 "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks," in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2014, pp. 1796–1801.

Aslan O and Samet, R 2020 "A comprehensive review on malware detection approaches," IEEE Access, vol. 8, pp. 6249–6271, 2020.

Aslan and A. A. Yılmaz, 2021 "A new malware classification frame- work based on deep learning algorithms," IEEE Access, vol. 9, pp. 87936–87951, 2021

Aslan, M. Ozkan-Okay, and D. Gupta, D 2021 "Intelligent behavior-based malware detection system on cloud computing environment," IEEE Access, vol. 9, pp. 83252–83271, 2021.

Bai Y and Kobayashi H 2003, "Intrusion detection systems: Technology and development," in Proc. 17th Int. Conf. Adv. Inf. Netw. Appl. (AINA), pp. 710–715.

Baykara and R. 2019 "SoftSwitch: A centralized honeypot-based secu- rity approach usingsoftware-defined switching for secure management of VLAN networks," TURKISH J.

Electr. Eng. Comput. Sci., vol. 27, no. 5, pp. 3309–3325, Sep. 2019.

Baykara K. and R. Das, N 2018 "A novel honeypot based security approach for real-time intrusion detection and prevention systems," J. Inf. Secur. Appl., vol. 41, pp. 103–116, Aug. 2018.

Bedi, N. Gupta, and V. Jindal, 2021"I-SiamIDS: An improved siam-IDS for handling class imbalance in network-based intrusion detection systems," Int. J. Speech Technol., vol. 51, no. 2, pp. 1133–1151, Feb. 2021.

Bhosale D.A and V. M. Mane, 2015 "Comparative study and analysis of network intrusion detection tools," in Proc. Int. Conf. Appl. Theor. Comput. Commun. Technol. (iCATccT), Oct. 2015, pp. 312–315.

Biermann E, Cloete, E.. and Venter L. M. 2020 "A comparison of intrusion detection systems," Comput. Secur., vol. 20, no. 8, pp. 676–683, Dec. 2001.

Boite, P.-A. Nardin, F. Rebecchi, M. Bouet, and Conan,V. 2017 "StateSec: Stateful monitoring for DDoS protection in software defined networks," in Proc. IEEE Conf. Netw. Softw. (NetSoft), Jul. 2017, pp. 1–9.

Boob and P. Jadhav, "Wireless intrusion detection system, 2010" Int. J. Comput. Appl., vol. 5, no. 8, pp. 9–13, 2010.

Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescape, 2020 "A hierarchical hybrid intrusion detection approach in IoT scenarios," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2020, pp. 1–7.

Byrnes, T. Hoang, N. N. Mehta, and Y. Cheng, 2020 "A modern implementation of system call sequence based host-based intrusion detection systems," in Proc. 2nd IEEE Int. Conf. Trust, Privacy Secur. Intell. Syst. Appl. (TPS-ISA), Oct. 2020, pp. 218–225.

Chawla, B. Lee, S. Fallon, and P. Jacob, 2018 "Host based intrusion detection system with combined CNN/RNN model," in Proc. Joint Eur. Conf. Mach. Learn. Knowl. Discovery Databases. Cham, Switzerland: Springer, Sep. 2018, pp. 149–158.

Choudhary S. and N. Kesswani,N 2021 "A hybrid classification approach for intrusion detection in IoT network," J. Sci. Ind. Res., vol. 80, no. 9, pp. 809–816, 2021.

Creech and J. Hu, 2014 "A semantic approach to host-based intrusion detec- tion systems using contiguousand discontiguous system call patterns," IEEE Trans. Comput., vol. 63, no. 4, pp. 807–819, Apr. 2014.

Creech, G 2014 "Developing a high-accuracy cross platform host-

based intrusion detection system capable of reliably detecting zero-day attacks," Ph.D. dissertation, School Eng. Inf. Technol., Univ. New South Wales, Canberra, ACT, Australia, 2014.

Deshpande, S. C. Sharma, S. K. Peddoju, and S. Junaid, 2018 "HIDS: A host based intrusion detection system for cloud computing environment," Int.J. Syst. Assurance Eng. Manage., vol. 9, no. 3, pp. 567–576, Jun. 2018.

Devan and N. Khare,2019 "An efficient XGBoost–DNN-based classification model for network intrusion detection system," Neural Comput. Appl., vol. 32, pp. 12499–12514, Jan. 2020.

Dwivedi, M. Vardhan, S. Tripathi, and A. K. Shukla, 2020 "Implementation of adaptive scheme in evolutionary technique for anomaly-based intrusion detection," Evol. Intell., vol. 13, no. 1, pp. 103–117, Mar. 2020.

Eskandari,M. Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," IEEE Internet Things J., vol. 7, no. 8, pp. 6882–6897, Aug. 2020.

Ethala K, R. Seshadri R, Renganathan N. G, and Saravanan M. S. 2013, "A role of intrusion detection system for wireless LAN using various schemes and related issues," Amer. J. Appl. Sci., vol. 10, no. 9, p. 979.

Farshchi J. (2003). Wireless Intrusion Detection Systems. [Online]. Available: http://www.securityfocus.com/infocus/1742

Fladby, H. Haugerud, S. Nichele, K. Begnum, and A. Yazidi, 2020 "Evading a machine learning-based intrusion detection system through adversarial perturbations," in Proc. Int. Conf. Res. Adapt. Convergent Syst., Oct. 2020, pp. 161–166.

García P. Eodoro T., Díaz Verdejo J., Maciá-Fernández G., and VázquezE. 2009 "Anomaly-based network intrusion detection: Techniques, systems and challenges," Comput. Secur., vol. 28, nos. 1–2, pp. 18–28, Feb. 2009.

Garuba M, Liu C, and Fraites D 2008, "Intrusion techniques: Comparative study of network intrusion detection systems," in Proc. 5th Int. Conf. Inf. Technol., New Generat. (ITNG), pp. 592–598.

Gassais, N. Ezzati-Jivan, J. M. Fernandez, D. Aloise, and M. R. Dagenais, 2020 "Multi-level host-based intrusion detection system for Internet of Things," J. Cloud Comput., vol. 9, no. 1, pp. 1–16,Dec. 2020.

Geramiraz F, A. S. Memaripour, and M. Abbaspour, 2012 "Adaptive anomaly- based intrusion

detection system using fuzzy controller," Int. J. Netw. Secur., vol. 14, no. 6, pp. 352–361, 2012.

Gunduz R 2020 "Cyber-security on smart grid: Threats and potential solutions," Comput. Netw., vol. 169, Mar. 2020, Art. no. 107094.

Gupta and R. Mamtora,2012 "Intrusion detection system using wireshark," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no. 11, pp. 358–363, 2012.

Hadem P., Saikia D.K, and Moulik S. 2021, "An SDN-based intrusion detection system using SVM with selective logging for IP traceback," Comput. Netw., vol. 191, May 2021, Art. no. 108015.

Han S, Xie M, Chen H.H, and Ling Y. 2014, "Intrusion detection in cyber- physical systems: Techniques and challenges," IEEE Syst. J., vol. 8, no. 4, pp. 1052–1062, Dec. 2014.

Han S.J. and S.-B. Cho, 2003 "Detecting intrusion with rule-based integration of multiple models," Comput. Secur., vol. 22, no. 7, pp. 613–623, Oct. 2003.

Harish B.S and S. A. Kumar, 2017 "Anomaly based intrusion detection using modified fuzzy clustering," Int. J. Interact. Multimedia Artif. Intell., vol. 4, no. 6, pp. 54–59, 2017.

Hick, E. Aben, K. Claffy, and Polterock. J.2012The CAIDA 'DDoS Attack 2007' Dataset. Accessed: Jun. 9, 2012. [Online]. Available: http://www.caida.org/data/passive/ddos-20070804dataset.xml

Hubballi N. and V. Suryanarayanan, 2014 "False alarm minimization tech- niques in signature-based intrusion detection systems: A survey," Comput. Commun., vol. 49, pp. 1–17, Aug. 2014.

Jyothsna V, Prasad R, and Prasad K.M 2011, "A review of anomaly based intrusion detection systems," Int. J. Comput. Appl.," vol. 28, no. 7, pp. 26–35.

Kang, K. McLaughlin, and S. Sezer, 2016 "Towards a stateful analysis framework for smart grid network intrusion detection," in Proc. 4th Int. Symp. ICS SCADA Cyber Secur. Res., Aug. 2016, pp. 124–131.

Karatas and Sahingoz, O.K 2018 "Neural network based intrusion detection systems with different training functions," in Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS), Mar. 2018, pp. 1–6.

Karthikeyan K.A and Indra, A 2010 "Intrusion detection tools and techniques—A survey," Int. J. Comput. Theory Eng., vol. 2, no. 6, p. 901,.

Kasongo and Y. Sun, 2019 "A deep learning method with filter based feature engineering for wireless intrusion detection

system," IEEE Access, vol. 7, pp. 38597–38607, 2019.

Kasongo and Y. Sun, 2020"A deep learning method with wrapper based feature extraction for wireless intrusion detection system," Comput. Secur., vol. 92, May 2020, Art. no. 101752.

Khan, A. T. 2021 "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," Processes, vol. 9, no. 5, p. 834, May 2021.

Khraisat A, Gondal I, Vamplew P, and Kamruzzaman J 2019, "Survey of intrusion detection systems: Techniques, datasets and challenges," Cybersecurity, vol. 2, no. 1, pp. 1–22, Dec. 2019.

Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, 2016 "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 184–208, 1st Quart., 2016.

Kolias, V. Kolias, and G. Kambourakis, 2017 "TermID: A distributed swarm intelligence-based approach for wireless intrusion detection," Int. J. Inf. Secur., vol. 16, no. 4, pp. 401–416, 2017.

Kruegel C, Valeur F, and Vigna G, 2004, Intrusion Detection and Correlation: Challenges and Solutions, vol. 14. Springer, 2004.

Kumar and O. P. Sangwan, 2012 "Signature based intrusion detection system using SNORT," Int. J. Comput. Appl. Inf. Technol., vol. 1, no. 3, pp. 35–41, Nov. 2012.

Kumar, A. Viinikainen, and Hamalainen, T 2016. "Machine learning classification model for network based intrusion detection system," in Proc. 11th Int. Conf. Internet Technol. Secured Trans. (ICITST), Dec. 2016, pp. 242–249.

Kumar, G. P. Gupta, and R. Tripathi, 2021 "Design of anomaly-based intrusion detection system using fog computing for IoT network," Autom. Control Comput. Sci., vol. 55, no. 2, pp. 137–147, Mar. 2021.

Lazarevic A, Kumar V, and Srivastava J 2005, "Intrusion detection: A survey," in Managing Cyber Threats. Boston, MA, USA: Springer,pp. 19–78.

Lim, T. S. Yer, J. Levine, and H. L. Owen,2003 "Wireless intrusion detection and response," in Proc. IEEE Syst., Man Cybern. Soc. Inf. Assurance Workshop, Jun. 2003, pp. 68–75.

Lydia Catherine, R. Pathak, and V. Vaidehi, 2014 "Efficient host based intrusion detection system using partial decision tree and correlation feature selection algorithm," in Proc.

Int. Conf. Recent Trends Inf. Technol., Apr. 2014, pp. 1–6.

M. Liu, Z. Xue, X. He, and J. Chen, 2021"SCADS: A scalable approach using spark in cloud for host-based intrusion detection system with system calls," 2021, arXiv:2109.11821.

Malek, B. Trivedi, and A. Shah, 2020 "User behavior pattern - Signature based intrusion detection," in Proc. 4th World Conf. Smart Trends Syst., Secur. Sustainability (WorldS4), Jul. 2020, pp. 549–552.

Mazini, B. Shirazi, and I. Mahdavi, 2019 "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms," J. King Saud Univ., Comput. Inf. Sci., vol. 31, no. 4, pp. 541–553, Oct. 2019.

Meftah, T. Rachidi, and N. Assem, 2019 "Network based intrusion detection using the UNSW-NB15 dataset," Int. J. Comput. Digit. Syst., vol. 8, no. 5, pp. 478–487, 2019.

Meng and Li, W 2013 "Evaluation of detecting malicious nodes using Bayesian model in wireless intrusion detection," in Proc. Int. Conf. Netw. Syst. Secur. Berlin, Germany: Springer, Jun. 2013, pp. 40–53.

Milenkoski A, Vieira M, Kounev S, Avritzer A, and Payne B.D 2015, "Evaluating computer intrusion detection systems: A survey of common practices," ACM Comput. Surv., vol. 48, no. 1, pp. 1–41.

Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, 2018 "Kitsune: An ensemble of autoencoders for online network intrusion detection," 2018, arXiv:1802.09089.

Moon, H. Im, I. Kim, and J. H. Park, 2017"DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks," J. Supercomput., vol. 73, no. 7, pp. 2881–2895, 2017.

More S, Mathews M.L, Joshi A, and Finin T 2012, "A semantic approach to situational awareness for intrusion detection," in Proc. Nat. Symp. Moving Target Res. (MTR). Baltimore, MD, USA: UMBC, 2012.

Moustafa N and J. Slay, J 2015 "UNSW-NB15: A comprehensive data set fornetwork intrusion detection systems (UNSW-NB15 network data set)," in Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), Nov. 2015, pp. 1–6.

Mudzingwa D and R. Agrawal,R 2012 "A study of methodologies used in intrusion detection and prevention systems (IDPS)," in Proc. IEEE Southeastcon, Mar. 2012, pp. 1–6.

Musa, M. Chhabra, A. Ali, and M. Kaur, '2020 'Intrusion detection system using machine learning techniques: A review," in Proc.

Int. Conf. Smart Electron. Commun. (ICOSEC), Sep. 2020, pp. 149–155.

Narsingyani D and O. Kale, 2015 "Optimizing false positive in anomaly based intrusion detection using genetic algorithm," in Proc. IEEE 3rd Int. Conf. MOOCs, Innov. Technol. Educ. (MITE), Oct. 2015, pp. 72–77.

Nitin, S. R. Singh, and P. G. Singh, 2012"Intrusion detection and prevention system (IDPS) technology-network behavior analysis system (NBAS)," ISCA J. Eng. Sci, vol. 1, no. 1, pp. 51–56, 2012.

OtoumU. and A. Nayak, 2021"AS-IDS: Anomaly and signature based IDS for the Internet of Things," J. Netw. Syst. Manage., vol. 29, no. 3, pp. 1–26, Jul. 2021.

Ou, Y. Lin, Y. Zhang, and Y.-J. Ou, 2010 "The design and implementation of host-based intrusion detection system," in Proc. 3rd Int. Symp. Intell. Inf. Technol. Secur. Informat., Apr. 2010, pp. 595–598.

Özgür Aand H. Erdem, 2010"A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015," PeerJ Preprints, vol. 4, Apr. 2016, Art. no. e1954v1.

OzkanOkay M, and Samet R2020, "Hybrid intrusion detection approach for wireless local area network," in Proc. 7th Int. Conf. Control Optim. Ind. Appl. (COIA), 2020, pp. 311–313.

Pacheco, V. Benitez, and L. Félix, 2019 "Anomaly behavior analysis for IoT network nodes," in Proc. 3rd Int. Conf. Future Netw. Distrib. Syst., Jul. 2019, pp. 1–6.

Park, S. Kim, H. Kwon, D. Shin, and D. Shin,2021 "Host-based intrusion detection model using Siamese network," IEEE Access, vol. 9, pp. 76614–76623, 2021.

Qassim, A. M. Zin, and M. J. A. Aziz, 2016"Anomalies classification approach for network-based intrusion detection system," Int. J. Netw. Secur., vol. 18, no. 6, pp. 1159–1172, 2016.

Qureshi, H. Larijani, J. Ahmad, and N. Mtetwa, 208"A novel random neural network based approach for intrusion detection systems," in Proc. 10th Comput. Sci. Electron. Eng. (CEEC), Sep. 2018, pp. 50–55.

Rai, M. S. Devi, and A. Guleria, 2016 "Decision tree based algorithm for intrusion detection," Int. J. Adv. Netw. Appl., vol. 7, no. 4, p. 2828, 2016.

Rashid, M. J. Siddique, and S. M. Ahmed, M. 2020 "Machine and deep learning based comparative analysis using hybrid approaches for intrusion detection system," in Proc. 3rd

Int. Conf. Adv. Comput. Sci. (ICACS), Feb. 2020, pp. 1–9.

Resmi A.M and R. Manicka, R 2017 "Intrusion detection system techniques and tools: A survey," Scholars J. Eng. Technol., vol. 5, no. 3, pp. 122–130, 2017.

Riyaz and S. Ganapathy, 2020 "A deep learning approach for effective intrusion detection in wireless networks using CNN," Soft Comput., vol. 24, no. 22, pp. 17265–17278, Nov. 2020.

Sabahi F and A. Movaghar A. 2008, "Intrusion detection: A survey," in Proc. 3rd Int. Conf. Syst. Netw. Commun., pp. 23–26.

Samrin N and D. Vasumathi, 2017 "Review on anomaly based network intru- sion detection system," in Proc. Int. Conf. Electr., Electron., Commun., Comput., Optim. Techn. (ICEECCOT), Dec. 2017, pp. 141–147.

Santos R.J, Bernardino J, and Vieira M.2014, "Approaches and challenges in database intrusion detection," ACM SIGMOD Rec., vol. 43, no. 3, pp. 36–47, Dec. 2014.

Satam and S. Hariri, 2021 "WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol," IEEE Trans. Netw. Service Manage., vol. 18, no. 1, pp. 1077–1091, Mar. 2021.

Sbai and M. El Boukhari, 2020 "Data flooding intrusion detection system for MANETs using deep learning approach," in Proc. 13th Int. Conf. Intell. Syst., Theories Appl., Sep. 2020, pp. 1–5.

Scarfone K and Mell P. 2007, Guide to Intrusion Detection and Prevention Systems (IDPS), Standard NIST SP 800-90,.

Seo, H. Lee, and E. Nuwere, 2013 "SIPAD: SIP-VoIP anomaly detection using a stateful rule tree," Comput. Commun., vol. 36, no. 3, pp. 562–574, 2013.

Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, 2018 "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. ICISSP, Jan. 2018, pp. 108–116.

Sharma, I. You, K. Yim, R. Chen, and J. H. Cho,H 2019 "BRIoT: Behavior rule specification-based misbehavior detection for IoT-embedded cyber- physical systems," IEEE Access, vol. 7, pp. 118556–118580, 2019.

Shon T and Moon, J 2024 "A hybrid machine learning approach to network anomaly detection," Inf. Sci., vol. 177, no. 18, pp. 3799–3821, Sep. 2024.

Singh, M. M. Singh, A. Sarkar, and J. K. Mandal,2021 "A novel wide & deep transfer learning stacked GRU framework for network intrusion detection," J. Inf. Secur. Appl., vol. 61, Sep. 2021, Art. no. 102899.

Snider, D. "A process to transfer Fail2ban data to an adaptive enterprise intrusion detection and prevention system," in Proc. SoutheastCon, Mar. 2016, pp. 1–4.

Sonule, M. Kalla, A. Jain, and D. Chouhan, 2020 "UNSW-NB15 dataset and machine learning based intrusion detection systems," Int. J. Eng. Adv. Technol., vol. 9, pp. 2638–2648.

Srivastav, P. Kumar, and R. Goel, 2013 "Evaluation of network intrusion detection system using PCA and NBA," Int. J. Adv. Res. Comput. Eng. Technol., vol. 2, no. 11, pp. 1–9, 2013.

Subba, S. Biswas, and S. Karmakar, 2017 "Host based intrusion detection system using frequency analysis of n-gram terms," in Proc. IEEE Region 10 Conf. (TENCON), Nov. 2017, pp. 2006–2011.

Tama,B. M. Comuzzi, and K. Rhee, '2019 'TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system," IEEE Access, vol. 7, pp. 94497–94507, 2019.

Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl., Jul. 2009, pp. 1–6.

Thakkar A and R. Lohiya, 2020 "A review of the advancement in intrusion detection datasets," Proc. Comput. Sci., vol. 167, pp. 636–645, Jan. 2020.

Thanthrige U. S. K. P. M., J. Samarabandu, and X. Wang, 2016 "Machinelearning techniques for intrusion detection on public dataset," in Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE), May 2016, pp. 1–4.

Timofte, J 2008 "Intrusion detection using open source tools," Inform. Econ.J., vol. 2, no. 46, pp. 75–79

Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, 2009 "Intrusion detection by machine learning: A review," Expert Syst. Appl., vol. 36, no. 10, pp. 11994–12000, 2009.

Uddin, A. A. Rahman, N. Uddin, J. Memon, R. A. Alsaqour, and S. Kazi, 2013"Signature-based multi-layer distributed intrusion detection system using mobile agents," Int. J. Netw. Secur., vol. 15, no. 2, pp. 97–105, 2013.

Verma, A. Bhandari, and G. Singh, G 2020 "Review of existing data sets for network intrusion detection system," Adv. Math., Sci. J., vol. 9, no. 6, pp. 3849–3854

Viegas, A. Santin, A. Bessani, and N. Neves, 2019 "BigFlow: Real-time and reliable anomaly-based intrusion detection for high-speed networks," Future Gener. Comput. Syst., vol. 93, pp. 473–485, Apr. 2019.

Vigna G and Kemmerer R.A 1999, "NetSTAT: A network-based intrusion detection system," J. Comput. Secur., vol. 7, no. 1, pp. 37–71, Jan. 1999.

Vijayakumar and S. Ganapathy, 2018 "Machine learning approach to combat false alarms in wireless intrusion detection system," Comput. Inf. Sci., vol. 11, no. 3, pp. 67–81, 2018.

Vinchurkar and A. Reshamwala, 2012 "A review of intrusion detection system using neural network and machine learning," Int. J. Eng. Sci. Innov. Technol., vol. 1, no. 2, pp. 54–63, 2012.

Wang, A. Kordas, L. Hu, M. Gaedke, and D. Smith, "Administrative evaluation of intrusion detection system," in Proc. 2nd Annu. Conf. Res. Inf. Technol., Oct. 2013, pp. 47–52.

Yang, K. McLaughlin, S. Sezer, Y. B. Yuan, and W. Huang, 2014 "Stateful intrusion detection for IEC 60870-5-104 SCADA security," in Proc. IEEE PES Gen. Meeting Conf. Expo., Jul. 2014, pp. 1–5.

Yang, S. 2021 "Research on network malicious behavior analysis based on deep learning," in Proc. IEEE 5th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC), Mar. 2021, pp. 2609–2612

Yassin, N. I. Udzir, Z. Muda, A. Abdullah, and M. T. Abdullah, 2012 "A cloud-based intrusion detection service framework," in Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic (CyberSec), Jun. 2012, pp. 213–218.

Yassin, N. I. Udzir, Z. Muda, and M. N. Sulaiman, 2013 "Anomaly- based intrusion detection through k-means clustering and Naives Bayes classification," in Proc. 4th Int. Conf. Comput. Informat. (ICOCI), vol. 49, Aug. 2013, pp. 298–303.

Ye, S. M. Emran, Q. Chen, and S. Vilbert, S 2002 "Multivariate statistical analysis of audit trails for host-based intrusion detection," IEEE Trans. Comput., vol. 51, no. 7, pp. 810–820, Jul. 2002.

Youssef and A. Emam, 2011"Network intrusion detection using data mining and network behaviour analysis," Int. J. Comput. Sci. Inf. Technol., vol. 3, no. 6, pp. 87–98, Dec. 2011.