INTRUSION DETECTION SYSTEM

Abstract:

Intrusion Detection Systems (IDS) are more important than ever in today's digital environment, where threats from cyberspace are ever evolving. in complexity and scope. IDS acts as a watchful defender of systems and networks, spotting illegal activity and policy infractions instantly and warning administrators before harm is done. IDS technologies have made great strides in detecting known and unexpected threats, moving from conventional signature-based systems to sophisticated anomaly detection techniques.

By allowing intelligent, automated threat detection capabilities that change over time, the pairing of artificial intelligence (AI) and machine learning (ML) has significantly improved IDS efficiency. Methods like ensemble techniques, deep learning models, and artificial immune systems provide strong instruments for identifying intricate attack patterns that could otherwise elude conventional security measures.

Depending on the system architecture and security needs, different IDS types—including Network-based (NIDS), Host-based (HIDS), Signature-based (SIDS), and Anomaly-based (AIDS)—offer customized protection. Furthermore, more precise defensive strategies are enabled by knowing the actions and intentions of various intruders, including masqueraders, misfeasors, and clandestine users.

To sum up, IDS is a proactive part of cybersecurity architecture rather than merely a reactive one. The tools and tactics used to identify and stop cyberattacks must advance along with the complexity of these assaults. IDS can offer a strong line of defense that guarantees the availability, confidentiality, and integrity of vital systems and data with the use of AI, adaptive models, and ongoing monitoring.

Introduction:

In network security systems, intrusion detection systems, or IDS for short, are commonly used. It is mainly used to find unusual and unauthorized network traffic patterns. IDS is necessary to protect data. Numerous automated security devices have been developed to protect the private information of businesses and organizations. Of these, intrusion detection systems (IDS) are the most effective.

When malicious transactions are found in network traffic, IDS keeps an eye out for them and immediately notifies users. It is software designed to look for malicious activity or policy violations on a network or system. An SIEM system typically logs all illegal behavior and violations centrally to prevent harmful conduct and protects a computer network from unauthorized users, including insiders.   
 IDSs are used to identify criminal users and hackers, as well as to stop their illegal access. It alerts the security administrator if it detects any behavioral anomalies. automated systems configured according to a person's wants and requirements. Intrusion detection systems (IDS) can identify patterns in networks, keep an eye on user behavior, spot unusual network activity, or ensure that system or user activity doesn't contravene operating policies.

Literature Review:

1. Security of network systems

It speaks about the procedures and tools used to safeguard private data. The CIA Triad (Confidentiality, Integrity, and Availability) is used in this context to protect sensitive data and computer networks. Protecting sensitive data from unwanted access, misuse, failure, or disturbance is the second iteration of cyber security.

Network system security fundamentals:

1. Firewalls.
2. The system that detects and prevents intrusions (IDS/IPs).

iii. Controlled Access Encryption

iv. VPN stands for virtual private networks.

v. Network Security Protocols for Segmentation

vi. Patch Control

vii. Keeping an eye on networks and recording

viii. Architecture Without Credibility

1. Data Protection:

Sensitive information is protected by data protection, which is a collection of techniques to prevent data loss, corruption, unlawful access, and misuse. Both privacy and cyber security depend on this. The CIA triad, which stands for confidentiality, integrity, and availability, is a set of principles that govern data protection.

1. CONFIDENTIALITY:

Guarantees that only authorized individuals can access important information. It stops data from being disclosed without authorization. Data classification, network security, access control, and encryption are some of the methods.

1. INTEGRITY:

Guarantees that during its existence, data will continue to be reliable, accurate, and consistent. It assists in stopping unwanted data alteration. Among the methods are audit logs, digital signatures, checksums, hashing, and version control.

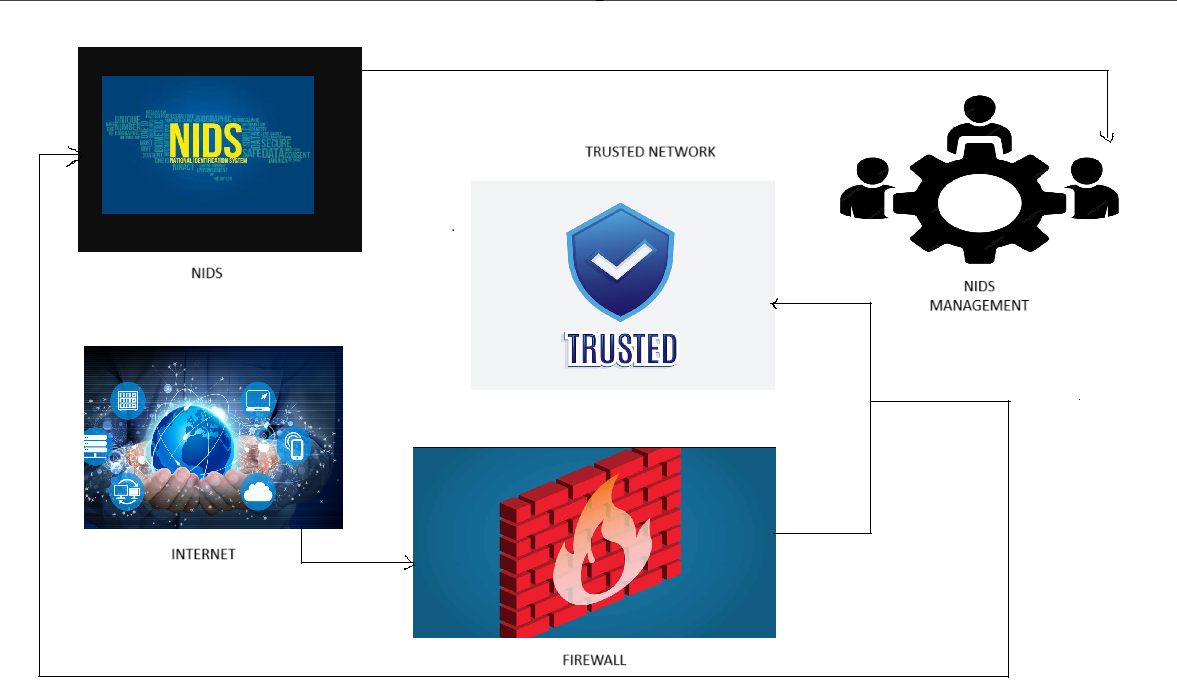
1. AVAILABILITY:

Guarantees that, when required, authorized individuals can access data and systems. It guarantees uninterrupted functioning and reduces downtime. Redundancy, disaster recovery and backup plans, DDoS defense, and system and network monitoring are some of the strategies.

DATA PROTECTION TECHNIQUES:

1. Encryption
2. Data Masking
3. Access Control
4. Data Loss Prevention (DLP)
5. Backup and Recovery
6. Data Classification
7. Tokenization
8. Anonymization and Pseudonymization
9. INTRUSION DETECTION SYSTEM:

Intrusion detection systems (IDS) are security solutions that keep an eye on system or network activity to spot malicious or questionable activity. IDS can assist in locating risks including malware, illegal access, and data breaches. IDS can alert security teams to potential risks, even if they usually don't stop them.



1. ATTACKS:

The two primary categories of attacks are malicious and selfish.

Selfish attacks:

Attackers who wish to use the spectrum with a higher priority are said to be committing selfish attacks. By tricking other unauthorized users into thinking he is a licensed user, this assault achieves its goal. Therefore, if the hostile user so desires, they can occupy the spectrum resource. This attack is referred because it violates the spectrum sharing plan. The CR network is susceptible to selfish assaults, in which self-centered SUs alters transmission parameters to improve their own utilities by impairing other users' performance, hence increasing their access probability. As a result, the CR network performs worse.

Malicious attack:

A malicious attack occurs when the adversary produces a denial of service (DoS) and stops other unlicensed users from using the spectrum. Malicious attacks will significantly reduce the available bandwidth and disrupt all traffic as a result. The situation described by Clancy and Goergen (2008) that turns a cognitive radio into a jammer is examined here. Assume that a PU is periodically evaluating a channel in a system. SUs can identify both primary and secondary users' channel access thanks to their channel sensing mechanism. Throughput T  
an interference I are balanced by their object function, which appears to

Where i the weight of the system participant. The technology aims to reduce interference and increase throughput.

b. WORKING OF INTRUSION DETECTION SYSTEM:

* An intrusion detection system (IDS) keeps an eye on network traffic to spot any questionable activities.
* To find trends and indications of unusual activity, it examines the data moving through the network.
* To find any activity that would point to an attack or intrusion, the IDS examines network activity against a set of pre-established rules and patterns.
* The system administrator receives an alert from the IDS if it finds something that fits one of these patterns or rules.
* After reviewing the notice, the system administrator can take appropriate action to stop any additional intrusion or harm.

c. ANAMOLY - BASED INTRUTION DETECTION SYSTEM:

By keeping an eye on system activity and categorizing it as either normal or abnormal, an anomaly-based intrusion detection system can identify computer and network invasions as well as misuse. The classification aims to identify any kind of misuse that interferes with regular system operation and is based on heuristics or rules rather than patterns or signatures. This contrasts with signature-based systems, which are limited to identifying attacks for which a signature has already been generated.

The system should be trained to detect typical system activities to positively identify attack traffic. The training phase and the testing phase are the two stages of many anomaly detection systems. There are various methods for identifying anomalies, but artificial intelligence-style methods are most frequently used. Artificial neural network-based systems have shown to be highly effective. Another approach is to use a rigorous mathematical model to define what constitutes regular system usage and to mark any variation from this as an attack. These are referred to as artificial immune systems and rigorous grammar-based approaches.

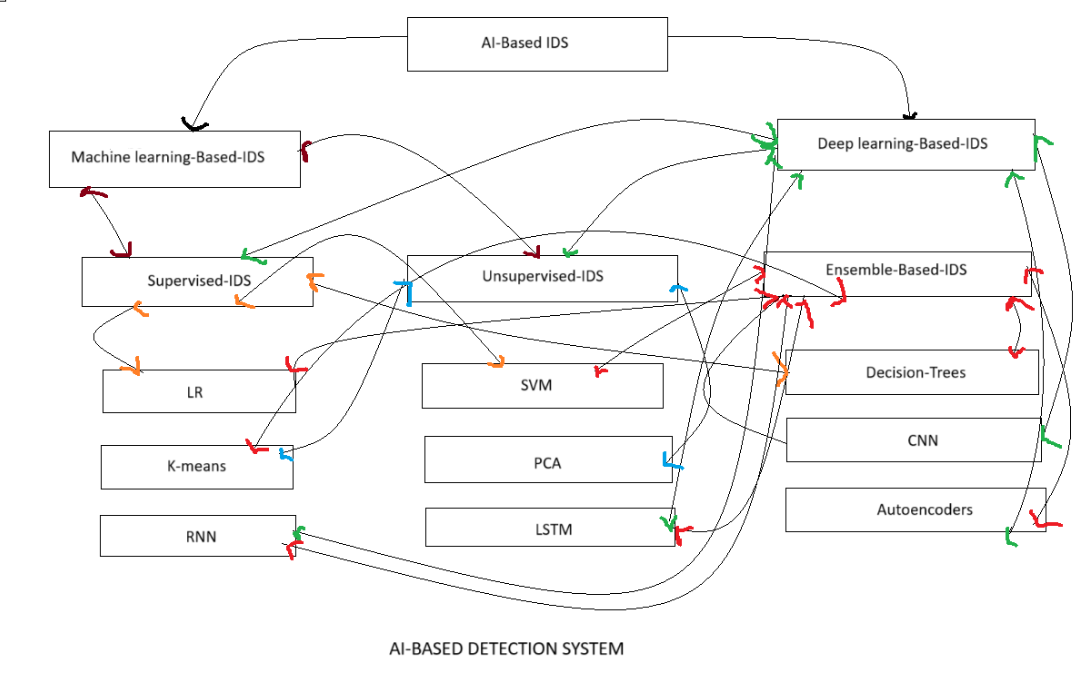
d. ARTIFICIAL INTELLIGENCE IN INTRUTION DETECTION SYSTEM:  
 The widespread usage of data and the internet makes security essential. Research has been going on to create an automated system that can identify unusual traffic. More sectors than ever before are moving to cloud computing since its introduction. Cybersecurity problems will also sharply rise in tandem with this trend. As a result, sufficient solutions are needed to guarantee that the network and cloud operate as intended. An appealing method for identifying and categorizing attacks is intrusion detection based on artificial intelligence.

If traditional technologies fail, an intrusion detection system (IDS) serves as a flexible layer of protection for network security. Its main objective is to identify network packets by critically examining them and to notify administrators by producing alarms. The IDS can identify binary and multiclass classifications since cloud infrastructure manages massive volumes of traffic and established solutions were unable to identify and categorize the attacks. In the case of binary, the model returns the label as either regular data or attack; in the case of multiclass, the output will be multivalued and contain a variety of attack types. Prevention skills can also be offered to avert potential incidents, which is the foundation of intrusion detection. Intrusion detection and prevention systems are the collective term for the mechanism.

The detection mechanisms can be divided into two categories: anomaly-based and signature-based. Intrusion detection systems that rely on signatures find patterns and compare them to the events that can be seen. The technique is insufficient, even though the system can identify every known assault because the patterns are different for identifying new attacks [18]. By identifying any departure from typical behavior, IDS systems can also identify anomalies. Another name for the system is abuse detection. Three components form the basis of the detection mechanism: detection, training, and parameterization. The parameterization process involves representing the observable behaviors, such as hosts and network connections. The training module is used to develop a classification model that categorizes these observed behaviors as either normal or aberrant.

A classification of AI-Based Intrusion Detection Systems (IDS) is shown in this graphic. It divides the many AI-based intrusion detection techniques—especially in cybersecurity—into three primary groups: ensemble-based intrusion detection systems, machine learning-based intruder detection systems, and deep learning-based intrusion detection systems.

Top Level: AI-Based Intrusion Detection Systems: These systems employ artificial intelligence to identify intrusions or cyberthreats.



An IDS Based on Machine Learning, these systems, which employ conventional machine learning techniques, are divided into:

* IDS under supervision: Trained on labeled data.
* Strategic Regression (LR)
* Support Vector Machine (SVM)
* Trees for Decisions
* IDS that is unsupervised: Trained on unlabeled data.
* K-means (a technique for clustering)

IDS Based on Deep Learning, these systems make use of deep learning architectures and neural networks:

* Convolutional neural networks, or CNNs, are frequently employed for structured features or geographical data.
* Sequential data is handled by recurrent neural networks, or RNNs.
* Long Short-Term Memory (LSTM) is an RNN type that works well with lengthy sequences.
* Autoencoders: Learn compressed representations to detect anomalies.

To enhance performance, ensemble-based intrusion detection systems integrate various learning techniques, such as deep learning and/or machine learning. Any of the techniques can be combined to improve accuracy and robustness. Depending on whether they are supervised, unsupervised, or deep learning models, each subclass is further linked to algorithms.

e. ARTIFICIAL IMMUNE SYSTEM:

A class of rule-based machine learning systems called artificial immune systems (AIS) are inspired by the principles and workings of the vertebrate immune system. The learning and memory characteristics of the immune system are typically the basis for the algorithms used in the computational techniques known as evolutionary computation and amorphous computation.

The structure and operation of the immune system are abstracted to computational systems in artificial immune systems (AIS), and computational problems in mathematics, engineering, and information technology are studied using these systems. Artificial intelligence (AIS) is a branch of natural computation and biologically inspired computers that focuses on machine learning. It is a subsection of artificial intelligence, which also covers artificial general intelligence. Artificial immune systems (AIS), which are adaptive systems, use theoretical immunology as well as observable immune activities, principles, and models to solve challenges.

AIS differs from theoretical biology and computational immunology, which focus on simulating immunology through mathematical and computational models to gain a better understanding of the immune system. Nevertheless, these models served as the foundation for AIS and remain a source of inspiration. Finally, unlike other disciplines like DNA computing, the study of the immune system as a computational substrate is not the focus of the AIS area.

TECHNIQUES:

* Clonal selection algorithm:

The clonal selection theory of acquired immunity serves as the inspiration for a family of algorithms known as affinity maturation, which describes how B and T cells gradually enhance their response to antigens. These algorithms concentrate on the Darwinian features of the theory, which cite somatic hypermutation as the source of variation, cell division as the source of reproduction, and the affinity of antigen–antibody interactions as the source of selection. Clonal selection methods, which are like the genetic algorithm minus the recombination operator and parallel hill climbing, are most frequently used in the optimization and pattern recognition areas.

* Negative selection algorithm:

The negative selection algorithm is based on the positive and negative selection processes that take place in the thymus as T cells mature, a process known as T cell tolerance. Negative selection is the process by which self-reacting cells—that is, T cells that may target and destroy own tissues—are recognized and eliminated (apoptosis). The classification and pattern recognition problem domains, where the issue space is characterized in the complement of existing knowledge, are commonly addressed by this family of methods. In an anomaly detection domain, for instance, the algorithm creates a set of exemplar pattern detectors that are trained on typical (non-anomalous) patterns to model and identify hidden or unusual patterns.

* Immune network algorithm:

Niels Kaj Jerne's idiotypic network theory, which explains how anti-idiotypic antibodies (antibodies that select for other antibodies) regulate the immune system, served as the inspiration for these algorithms. Using antibodies (or cells that produce antibodies) as nodes, this family of algorithms focuses on the network graph structures involved. The training method grows or prunes the edges between the nodes according to affinity (similarity in the issue representation space). Like artificial neural networks, immune network methods have been applied in the fields of grouping, data visualization, control, and optimization.

* Dendritic cell algorithm:

Immune-inspired algorithms like the Dendritic Cell Algorithm (DCA) are developed using a multi-scale approach. This technique is based on an abstract model of dendritic cells (DCs). The DCA is designed by analyzing and simulating various aspects of DC functionality, including both the collective behavior of cell populations and the internal molecular mechanisms within individual cells. The algorithm processes information across multiple levels of granularity, which is achieved through multi-scale processing.

f. TYPES OF PROTECTION IN IDS:

IDS systems, like other systems, are available in a variety of flavors and possess varying capacities to identify any threats or questionable actions through a variety of techniques, such as

* NIDS system:

Network intrusion detection systems, or NIDS systems, are installed at critical locations throughout your company's network. It can now keep an eye on all network device traffic, both coming in and going out.

* HIDS system:

This is a host intrusion detection system that is installed on every computer or device connected to the network and provides direct access to the internet and the internal network of the company. Using a HIDS rather than a NIDS has several benefits since it may identify unusual network packets coming from inside the company as well as malicious traffic or activity that a NIDS system is unable to identify. An intrusion detection system (HIDS) can also detect harmful activity coming from the host, such as when malware is infected on the host and trying to propagate to other systems.

* SIDS system:

Like how antivirus software operates, this signature-based intrusion detection system may monitor every packet that moves over the network and compare it to a database of known dangerous threat features or attack signatures.

* AIDS system:

This is referred to as the anomaly-based intrusion detection system, which is known to monitor network traffic and compare it to a predetermined baseline to ascertain what constitutes typical network activity in terms of protocols, bandwidth, other devices, and ports. This kind of intrusion detection system uses machine learning to create a baseline and the security policy that goes with it. The IT teams receive an alert when the system detects any suspicious activity or policy infractions. The IDS system is anomaly-based, which helps to overcome the drawbacks of signature-based techniques, particularly when identifying new threats, by identifying these threats using a general model rather than traits and signatures.

g. TYPES OF INTRUDERS IN IDS:  
 The most damaging elements causing security weakness are intruders, often known as hackers. They possess vast knowledge and a thorough comprehension of security and technology. Users' privacy is violated by intruders who seek to steal their private information. After being stolen, the data is sold to third parties with the intention of abusing it for their own or their careers' benefit.

* Masquerader:

The term "masquerader" refers to the group of people who are not permitted to use the system but take advantage of users' privacy and sensitive data by using methods that allow them to take control of it. Masqueraders attempt to attack unethically to steal data because they are outsiders and do not have direct access to the system.

* Misfeasor:

The group of people who are permitted to use the system but abuse their privileges and access. These are the people that abuse the access and rights that have been granted to them; they are known as misfeasors. Insiders with direct access to the system are known as misfeasors, and they work to use it unethically to steal data and information.

* Clandestine User:

People who are permitted to use the system but abuse their privileges and access fall into this group. These people are known as misfeasors because they unlawfully abuse the access and rights that have been granted to them. Because they have direct access to the system and are insiders, misfeasors seek to exploit it unethically to steal data or information.

h. WAYS OF INTRUDERS:

* Try any short password that would allow them to access the system in a regressive manner.
* Try using the default passwords to unlock the system; if the user hasn't changed the default password, this will open the system.
* Try using the user's personal information, including their name, family members' names, address, and phone number, in various combinations to unlock the system.
* Utilizing a Trojan horse to gain access to the user's machine. Gaining access through their connection gateway and attacking the host's and remote user's connection.
* Attempting to get all the information that is pertinent to the user, including room numbers, license plate numbers, and local information.

1. MACHINE LEARNING IN INTRUSION DETECTION SYSTEM:

When modeling algorithms, artificial intelligence—primarily machine learning technologies—takes learning styles into account. The characteristic of the supplied data makes it a perfect fit for the algorithm's classification. ML primarily provides supervised and unsupervised classification algorithms that rely on the available training data. Teacher-student connections can be used to teach supervised learning, where the labeled dataset is classified and the training dataset is used to train the target dataset. One of the main methods in anomaly detection, supervised learning produces accurate results in intrusion detection categorization tasks. Every industry uses machine learning. The researchers have already presented several taxonomies for intrusion detection based on learning styles. There are training and testing steps in the classification process. Every industry uses machine learning. The researchers have already presented a few taxonomies for intrusion detection based on learning styles. There are training and testing steps in the classification process.

Intrusion detection using supervised machine learning, An ML job uses the relationships between input-output pairs to map output data. We have examined popular machine algorithms for intrusion detection for empirical study. Reaching a certain objective based on the training samples is the primary purpose of the supervised learning approach. Regression mechanisms and classification are the most prevalent tasks for this learning approach.

A support vector machine, SVM is a classification method that produces cutting-edge results in both classification and prediction, and it is a fundamental model in machine learning literature. Building a high-dimensional feature space from the input vectors in terms of the hyperplane and classifying them into positive and negative categories is the fundamental concept of support vector machines (SVM). Negative data indicates anomalous data, while positive data indicates typical data. A unique two-stage technique based on statistically based IDS. Two subgroups are created from the complete KDDcup99 dataset using the suggested method, which is based on the least squares SVM. The suggested method first chooses subsets of samples from the subgroups. The study also looked at an ideal allocation plan based on the subgroup's vulnerabilities. The samples will then be extracted using the suggested method for intrusion detection. SVM is used to choose the features in Ref. [22], which improves the classification accuracy of all attacks.

Regression analysis using logistic methods, one of the supervised techniques utilized for both binary and multiclass classification applications is logistic regression. The idea behind logistic regression is to use the concept of probability to forecast the likelihood of an event. The application of logistic regression extends beyond the realm of intrusion detection to include areas such as spam detection [23]. suggested a unique method for IDS based on logistic regression and the genetic algorithm. Before beginning the classification process, the dataset's features are reduced using the genetic algorithm and the suggested best feature set selection approach. The logistic regression (LR) algorithm then categorizes the NSL-KDD dataset into distinct assaults after the suggested feature selection approach chooses the best feature based on the fitness score. The outcome demonstrated how well GA-BFSS performed logistic regression by reducing the number of features using the LR technique. In comparison to the current sophisticated supervised machine learning techniques, another study [24] found that LR-based intrusion detection systems and linear discriminant analysis performed better for binary and multi-class classification.

The Bayesian, it was within the framework of supervised learning that the Bayesian classification was created. The prediction of feature likelihood from the data is the foundation of an approach. To categorize, it uses the Bayes Theorem to calculate the likelihood based on the probability. Most research has been utilized to identify anomalous traffic to detect network penetration. We created a novel method for IDS in Ref. [26] that was based on the infinite bounded mixture model and Bayesian. The model was created to offer Internet of Things security. This technique selects features using a Bayesian approach, which has been mostly used for feature selection and parameter estimation, on an infinite bounded mixture model. Training uses samples from the full dataset, while testing uses the entire dataset. Finding the K-best BN structures based on the training data is the next phase, which is followed by data discretization on the testing and training data. Each network's conditional probability distribution is estimated using Bayesian estimation to produce K- independent BN classifiers, which are then applied to the training data. On the NSL-KDD dataset, the study's findings demonstrated good accuracy.

The algorithm of random forest, the algorithm in this supervised approach primarily uses multiple decision trees, one of the fundamental models in machine learning architecture. Multiple decision trees' prediction outputs are employed to forecast the ultimate result rather than just one decision tree. Due to its ensemble method foundation, Random Forest is a strong contender for effectively identifying threats on networks and in the cloud. Summarizes the several methods that have been suggested to improve intrusion detection. Using the DARPA dataset, the author also contrasts several classifiers for intrusion detection. As a result, compared to other models, the random forest offers greater categorization benefits. Despite taking longer than other classifiers, the random forest model has comparable intrusion detection performance. In the context of real-world applications, Random Forest is hence undesirable for real-time intrusion detection applications.

1. TYPES OF INTRUSION SYSTEM:

Anomaly-Based Intrusion Detection System (IDS):

An anomaly-based IDS identifies potential threats by detecting deviations from established patterns of normal behavior within a network or system. It begins by creating a baseline through statistical analysis of typical network traffic or system activity over time. Once this baseline is set, the IDS continuously monitors real-time activity and compares it to the norm. Any significant deviation is flagged as a possible intrusion, potentially indicating a previously unknown or evolving threat.

Signature-Based Intrusion Detection System (IDS):

A signature-based IDS detects threats by comparing network or system activity against a database of known attack signatures. These signatures are predefined patterns that correspond to specific types of malicious behavior. When the IDS identifies activity that matches one of these signatures, it triggers an alert, indicating a likely intrusion attempt. This technique works quite well for identifying recognized hazards.

Hybrid Intrusion Detection System (IDS):

A hybrid IDS integrates both anomaly-based and signature-based detection techniques to provide comprehensive protection. It utilizes signature-based methods to quickly identify known attacks, while anomaly-based methods help detect new, previously unseen threats. By combining these approaches, hybrid IDSs enhance detection accuracy and broaden coverage against a wide range of cyber threats.

1. CASE STUDY OF IDS:

A strong case study in the realm of Intrusion Detection Systems (IDS) is the deployment of the Bro IDS (now known as Zeek) at the Lawrence Berkeley National Laboratory (LBNL). Vern Paxson's 1999 documentation of this case serves as a fundamental illustration of how to construct an intrusion detection system in a high-stakes, high-traffic setting. LBNL, being a major U.S. research facility with a complex and high-speed network infrastructure, needed an IDS capable of detecting a wide variety of threats in real time without causing performance degradation or generating excessive false positives.

Bro was developed with a unique approach that separated it from traditional signature-based IDS systems. Instead of relying solely on predefined attack patterns, Bro used a policy-driven framework capable of deep packet inspection and protocol-level analysis. It monitored network activity in real time, identified unusual behaviors, and allowed custom scripts to define site-specific detection policies. This flexibility enabled security teams to adapt Bro to the evolving threat landscape and their specific network requirements.

One of the most impressive aspects of this deployment was Bro’s scalability. It successfully operated at multi-gigabit speeds while inspecting complete packet payloads, something many IDS systems at the time struggled to do. Furthermore, it was effective at detecting stealthy reconnaissance scans, application-layer attacks, and backdoors that were missed by simpler IDS tools. The system’s ability to log detailed events and correlate suspicious behaviors gave network administrators a clearer picture of security incidents as they unfolded.

This case study is particularly valuable because Bro was released as an open-source project, allowing other organizations to adopt and adapt it for their own use. Over time, it evolved into Zeek, which remains one of the most respected and widely used network security monitoring platforms in both academia and industry. The LBNL deployment of Bro is not just a success story of IDS effectiveness—it also exemplifies how research-driven solutions can have a lasting impact on real-world cybersecurity practices.

DISCUSSION:

A key component of contemporary cybersecurity architecture, intrusion detection systems (IDS) are crucial for spotting and stopping illegal or unusual activity in networked systems. Our investigation of artificial intelligence methods, artificial immune systems, and anomaly-based intrusion detection systems shows a substantial shift away from conventional security models and toward more flexible and dynamic solutions.

The growing importance of AI-based IDS, particularly those that use machine learning and deep learning, is one important discovery. These systems provide scalable solutions for big, complicated environments like cloud infrastructure, and they also perform better than signature-based IDS in identifying assaults that haven't been detected yet. This supports earlier research that indicates both supervised and unsupervised machine learning algorithms improve detection rates while lowering false positives. For example, our data confirms the use of recurrent neural networks (RNNs) and convolutional neural networks (CNNs) to increase classification accuracy in previous works.

Anomaly-based and AI-enhanced intrusion detection systems (IDS) provide real-time, self-learning capabilities, in contrast to previous models that only used pattern recognition or static rule sets. This change is particularly important as attackers are using more sophisticated strategies to get around established systems. For instance, the use of Artificial Immune Systems (AIS) such as the dendritic cell algorithm or clonal selection algorithm offers biologically inspired solutions that can recognize complicated patterns and learn adaptively, which was not possible with older IDS.

Nevertheless, AI-based systems present new difficulties in spite of their advantages. The need for high-quality, labeled training data in supervised models is a major drawback. Such datasets might not always be accessible or might not generalize well across various network conditions in real-world applications. Furthermore, deep learning models' resource requirements and computational complexity can be prohibitive, particularly for small businesses or edge devices with constrained processing capacity.

The possibility of hostile attacks is another issue. Future study on adversarial robustness is necessary since attackers can modify input data to trick AI-based IDS. Furthermore, explainability is still a problem; a lot of AI models function as "black boxes," making it hard for cybersecurity experts to understand the reasoning behind a detection or alarm.

In conclusion, even though the combination of machine learning and biologically inspired models has greatly improved intrusion detection systems, more work is required to ensure data quality, computational efficiency, interpretability, and protection from hostile manipulation. These observations support earlier research and point out areas where IDS technology has to advance to stay up with the quickly shifting cybersecurity environment.

CONCLUSION:

Intrusion Detection Systems (IDS) have become more and more important in a time when digital infrastructure serves as the foundation for essential services and corporate operations. IDS technology reduces the danger of data breaches, system abuse, and cyberattacks by acting as a watchful guardian over network environments and spotting unauthorized or unusual behavior.

This study examined several IDS facets, starting with conventional detection techniques including anomaly-based and signature-based methods. It emphasized how artificial intelligence and machine learning—including deep learning and artificial immune systems—are transforming intrusion detection systems (IDS) capabilities by making threat detection more accurate, dynamic, and adaptive.

Additionally, we discussed the need of safeguarding sensitive information using the CIA triad—confidentiality, integrity, and availability—and described the various kinds of intrusion detection systems and the variety of threats they must fend against. The study also highlighted how intrusion detection systems (IDS) have evolved from passive alert systems to proactive defense mechanisms by combining with security information and event management (SIEM) and intrusion prevention systems (IPS) tools.

IDS still have drawbacks despite the improvements, such as the high rate of false positives in anomaly detection, the difficulty of spotting zero-day attacks in signature-based systems, and the difficulty of keeping AI-based models' training data current. The necessity for ongoing innovation and hybrid solutions is further highlighted by the fact that skilled attackers are always coming up with new ways to avoid detection.