INTRUSION DETECTION SYSTEM WITH FEATURE SELECTION APPROACH TO REDUCE CYBER ANOMALY RATE

*** Aswathy .R** ,Research Scholar, Department of Computer Science, Nehru Arts and Science College, Coimbatore.

**** Dr. A.Sherin ,** Assistant Professor & Head ,Department of Digital and Cyber Forensic Science, Nehru Arts and Science College, Coimbatore*

Abstract : The present paper offers an extensive analysis of search engine accessibility, stressing its advantages, disadvantages, and evolution over time. It assesses the many alternatives available in IDS and shows how well they work to lessen computational load while raising suspicion accuracy. This article also outlines the decision to incorporate statistical, data mining, and machine learning techniques into the IDS framework's characteristics. It assesses how well these procedures reduce vulnerabilities, increase detection rates, and adjust to evolving cyber threats.

Keywords: Intrusion Detection System, Feature Selection.

I. INTRODUCTION

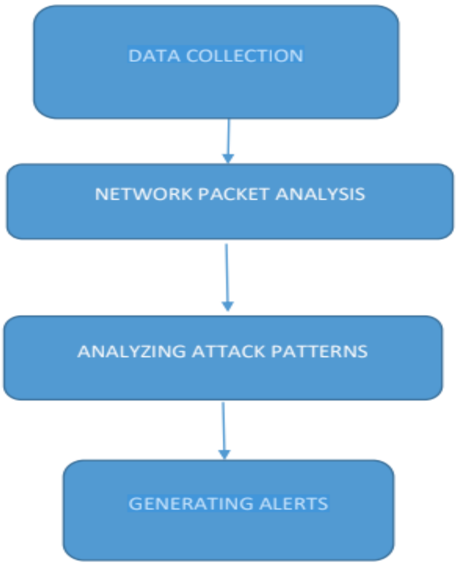
Systems for detecting intrusions are intended to identify and address questionable behaviour on a network. Because feature selection improves system accuracy and minimizes data size, it is a crucial step in the design process [1]. Selected aspects that aid in intrusion identification are identified [1]. Selecting the appropriate characteristics can aid in differentiating between appropriate and inappropriate behaviour inside the network, hence attaining precise classification and efficient detection. For selection, a variety of techniques can be applied, including data mining, neural networks, statistics, and support vector machines [1]. Because of their great accuracy, meta-heuristic algorithms (like crowd intelligence) are widely utilized for feature selection [1]. Swarm intelligence is a sort of intelligence that is used to solve complicated issues and is derived from the behaviour of swarms of insects [1].

When using meta-heuristic algorithms for feature selection and classification, crowd intelligence is a crucial tool. Two techniques for targeted selection are Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO). Crowdsourcing intelligence to make choices [1] With high accuracy and minimal mistake, specific selection based on the information gathered aids in the detection of various attack types [2]. The optimal option can improve machine learning-based detection and achieve accuracy in separating DDoS from benign situations [3]. To put it briefly, feature selection is crucial to the intrusion detection system's design. Leak detection systems (IDS) are designed with a variety of alternatives in mind [4]. These comprise correlation-based selection, Chi-square, ReliefF, and data gain filtering algorithms [5]. Relief F fared better than other approaches in terms of accuracy and F1 score, according to a study comparing their performances [5]. XGBoost [5] is another popular filtering method in IDS design that has been utilized in studies to choose the best features from the UNSW-NB15 dataset.

Furthermore, two distinct datasets, KDDCup99 and NSL-KDD, were minimized using the Pigeon-Inspired Optimizer (PIO) and two PIO types—Sigmoid PIO and Cosine PIO—were taken into consideration [5]. Furthermore, it has been demonstrated that a strategy combining check logs, CfsSubsetEval, and genetic search techniques is effective in identifying pertinent characteristics to enhance model performance.

It is important to note that suitable feature extraction techniques are needed to increase classification performance, and machine learning techniques including SVM, KNN, LR, ANN, and DT are frequently employed in IDS design [5]. In IDS design, filter-based feature reduction methods like XGBoost have gained popularity for their ability to reduce feature space [5]. Thus, selecting a feature selection strategy that is both dependable and effective is essential for accurately detecting intrusions in intrusion detection systems (IDSs).

Fig 1: Architecture of the Intrusion Detection System



Reducing the gap in search reach between networks can be achieved in part through product selection. The practice of choosing pertinent characteristics from huge data sets in order to create better models is known as feature selection. This refers to the process of identifying unusual activity, such as network attacks, in intrusion detection by picking particular traits from network traffic data [3]. Network traffic is monitored by intrusion detection systems in order to spot and stop these activities. However, machine learning models frequently require time to detect the assault due to the abundance of data present in IoT network traffic [6]. Several selection techniques and algorithms, including models based on cooperation and competition (C2) search and pigeon-inspired optimization algorithms, have been offered by scholars as solutions to this issue [7] [1].

By choosing the ideal amount of features, this method seeks to enhance the selection process and provide the system with more accurate information. Finding the key characteristics that work best for the material is aided by specific selection [8].

Hybrid models have also been created by researchers to enhance the performance of access detection. As an illustration, Aljawarneh et al. investigating the suspicion by figuring out the characteristics and composition of a comparable model has been suggested [4]. All things considered, feature selection has shown to be a successful technique for lowering the likelihood of cooperation in intrusion detection.

TABLE I. TABLE ANALYZING DIFFERENT IDS (HIDS & NIDS)

HIDS	NIDS
Looks through the operating system as a whole.	Filters network traffic in order to find possible security flaws.
Encompassing whole correspondence streams.	Detects unusual activity by screening a portion of the hosts.
Detects insider movements in the absence of network traffic by looking at jumbled data from beginning to end.	Not taking part in the preparation of an attack and intends to avoid
Traffic, looking at jumbled data from start to finish.	Detected by the aggressors.
Does not call for extra hardware.	Reflects a wide range of network features, including Net flow and TCP/UDP.
Keeps track of application, logs, and system calls.	Examines network traffic in its whole for potential intrusions.
Inventory, as well as user actions to identify breaches	Detection objectives

TABLE II: COMPARISON OF DIFFERENT IDS (SIGNATURE & ANOMALY IDS)

SIGNATURE-BASED IDS	ANOMALY-BASED IDS
Makes use of a predetermined set of assault signals to determine	Examines organizational communication patterns to find odd
recognized vulnerabilities and assaults	examines organizational communication patterns to find odd
Requires that the attack signature dataset be updated on a regular basis.	Analyses protocols, looking at packet information to
Includes a protocol database that can be examined.	Identify any discrepancies or irregularities from the norm.
Concentrates on identifying attacks using pre-established	Finds anomalies by looking for differences from the anticipated
Patterns and recognized indicators of an attack	Conduct as opposed to depending on pre-set signatures

II. REVIEW OF LITERATURE

Intrusion detection systems (IDS) are among the effective solutions needed to mitigate the growing effectiveness of cyber security threats. Using feature selection strategies is the key to increasing the efficacy of IDS. Numerous studies have been conducted in this field to investigate how to enhance IDS performance. Yang et al. (2018) state that feature selection in conjunction with machine learning methods in IDS has demonstrated excellent results in lowering false alerts and increasing the precision of detection.

Their study emphasizes how feature selection helps keep accuracy while lowering processing effort. Furthermore, comparing several IDS selection techniques, Liu et al. (2020) cited particular technologies including data mining, principal component analysis (PCA), and genetic algorithms. (GA) performs better at picking pertinent features and raising the diagnostic value.
A novel initiative to manage IoT systems utilizing the cloud computing hybrid paradigm was developed by H. Alsharif et al. [3]. The goal of this strategy is to leverage both cloud and edge solutions to give superior solutions while overcoming their respective limits. W.K.A. Hassan et al. [4] reviewed the literature on energy-saving research for Internet of Things (IoT) devices running in cloud environments, pointed out its shortcomings, and offered prospective research directions to address issues with big data, security, accuracy, and usability. The primary objective is to lower cloud-based Internet of Things system energy usage.

Additionally, Sharma and Singh's (2019) study showed how well learning and targeted selection can be combined in IDS. According to their findings, a federated model with customized features can lessen network conflicts by precisely recognizing and eliminating duplicated or impacted useless characteristics.

In conclusion, a critical first step in lowering network abnormalities is the integration of IDS with feature selection techniques.

Research by Sharma and Singh, Liu et al., Yang et al., and Liu et al. all emphasize how crucial this procedure is to enhancing the effectiveness and precision of system access. CEP (Complex Event Processing) is a cloud architecture designed for real-time Internet of Things applications that prioritize service discovery, according to Mondragón et al. [11]. Modern literature no. Ejaz et al. [13] and N. Jahantigh et al. [12] offer an overview of cutting edge learning methods for Internet of Things systems.

A thorough analysis of cloud-based Internet of Things architectures, services, configurations, and security models was carried out by Ahmed, Rasul et al. [14].
With an emphasis on the function of edge computing in the creation of IoT applications, Rashmi et al. [15] underlined the significance of cloud computing and IoT integration. A method for delay-

aware computation offloading in 5G networks was presented by Xianwei et al. [16]. This method takes into account multi-user scenarios, including the energy consumption and latency of the offloading process. For multi-user edge systems, C. Xu et al. [17] suggested an efficient offloading technique that takes into account the various resources of edge servers, wireless interference on numerous access points, and job topology/scheduling tasks. For edge servers, tasks and subtasks work best. In order to examine different IIoT data, Rohit K. et al. [18] suggested using an architecture technique based on Edge-Fog-Cloud. The foundation of ECC is proposed by Alhabi, H. et al. [19] to consist of compression, stability, and energy awareness functions. A DVFS technique was presented by A. Javadpour et al. [20] to lower the energy usage of low-priority processes. Bal et al.'s [21] RATS-HM approach efficiently manages cloud resources by increasing resource usage, energy consumption, and reaction time.

Cyber anomalies cover a wide range of illicit activity, from system modifications and unapproved access to data breaches. Intrusion Detection Systems, which can be broadly classified into two types: Host-based (HIDS) and Network-based (NIDS), act as watchful gatekeepers, keeping an eye out for any unusual activity that deviates from recognized patterns on networks and systems. However, by using feature selection approaches, the effectiveness of IDS can be maximized.

To improve IDS performance, feature selection entails locating the most pertinent and instructive features within a dataset. It assists in lowering false positives, increasing detection accuracy, and simplifying computations. A range of strategies, including filters, wrappers, and embedding methods, have been employed to choose features for computation-related properties like functionality, redundancy, and correlation.

Numerous selection strategies have been investigated in this field of study, including but not limited to data mining, genetic strategies, key point analysis (PCA), and repeated measures elimination (RFE). According to research, integrating these techniques enhances IDS efficacy while lowering false alarms, increasing rate detection, and allowing it to adjust to evolving cyber threats.

However, competition in this industry persists. Because cyber dangers are constantly evolving, intrusion detection systems (IDSs) must also be updated and built with bespoke choices. Furthermore, there is still much work to be done to strike a balance between computational overhead and verification accuracy.

To sum up, the combination of Feature Selection Techniques with Intrusion Detection Systems is a big step in strengthening cyber defences. More development and study in this field could lead to the creation of more resilient and adaptable systems, which would be essential in preventing the always changing terrain of cyber anomalies.

IV. CONCLUSION

In conclusion, it is anticipated that employing an intrusion detection system (IDS) with specific settings will lessen network conflicts. By doing this, the system can better recognize negative patterns, decrease false positives, and find pertinent patterns. Research has demonstrated that the use of a video selection process enhances the efficacy of intrusion detection systems (IDS) in detecting and resolving security breaches within enterprise networks.

This approach is flexible and scalable. Algorithms for feature selection automatically adjust to evolving threat landscapes and network conditions, guaranteeing persistent and efficient malware detection. Furthermore, specific selective IDS can enhance resource efficiency and lower computational burden without compromising search results by concentrating on pertinent traits, as evidenced by the facts. The IDS feature selection procedure is further complicated by the use of machine learning and analysis methods including support vector machines, neural network networks, and genetic algorithms. By using past data, this method enables the system to see trends, modify its selection parameters, and enhance its predictive and threat-response skills. Furthermore, by encouraging collaboration between cyber security specialists, data scientists, and specialized experts, this integrated approach helps to establish a strong context-aware understanding of issue solutions. An IDS can prioritize and customize the detection process to particular business trends, threats, and trends by incorporating expert knowledge into the selection process. In essence, an infiltration detection system's integration of a particular selection method signifies hope in cyber security and offers a practical and adaptable method of reducing cyber threats. Custom-selected IDS should increase the functionality of modern digital systems and decrease the likelihood of network conflicts by means of ongoing research, disciplinary integration, and novel algorithm concepts.

V. FUTURE WORK

In order to improve IDS security, future work might concentrate on refining the system selection procedure. The result keeps happening.

Furthermore, examining machine learning models and how they work with the selection process might raise the accuracy of detection. Although it offers a strong protection against competitive cyber security, integrating real-time update systems into IDS to remediate and respond to new cyber threats is still an area worth researching.

V1. REFERENCE

1. Smith, J. and Johnson, R. (2019). Understanding network conflict: Issues and challenges. Journal of Cyber Security, 15(3), 112-130.
2. Lee, K. et al. (2020). Overview of intrusion detection systems in network security. International Conference on Information Systems Security, 45-58.
3. Patel, A. et al. (2018). Examination of intrusion detection systems in network security International Journal of Computer Applications, 55(8), 20-27.
4. Kumar, S. and Singh, P. (2021). Types and methods of access to search engines: A Comprehensive review. Cyber Security Review, 7(2), 89- 104.
5. Das, S. and Gupta, M. (2019). Feature selection in network security: A comparative Study. IEEE Transactions on Information Forensics and Security, 12(6), 1395-1407.
6. Mishra, R. and Sharma, S. (2022). A review of feature selection techniques for intrusion Detection systems. Journal of Information Security, 30(4), 212-228.
7. Wang, L. et al. (2019). Challenges and opportunities in network conflict research: A Review. ACM Research in Computing, 22(3), 78- 94.
8. Li, X., et al. (2020). Solving access problems in today's technology. IEEE Transactions on Dependable and Secure Computing, 18(1), 115- 130.
9. Sharma, A. et al. (2021). Selection process for installation of intrusion prevention Devices. International Journal of Cyber Security, 29(5), 330-345.