Improving credibility, Setting up a cloud Intrusion Detection System and Fuzzy Neural Network

V. Selvakkumaran[1], R. Anandan[2]

[1]Reserarch Scholar , Supervisor School of Engineering, Department of Computer Science and Engineeering, Vels Institute of Science, Technology and Advanced Studies, (VISTAS) Deemed to be University Pallavaram, Chennai, Tamil Nadu, India
[2] Professor&Research Supervisor School of Engineering, Department of Computer Science and Engineeering, Vels Institute of Science, Technology and Advanced Studies, (VISTAS) Deemed to be University Pallavaram, Chennai, Tamil Nadu, India

Received: 14.04.2024 Revised : 16.05.2024 Accepted: 21.05.2024

ABSTRACT
In the constantly evolving field of cloud computing, ensuring the security and dependability of services is crucial. This research presents a novel method of detecting intrusions in cloud systems using the integration of neural networks with fuzzy logic. The Fuzzy Neural Network Aided Cloud Intrusion Detection System (FNN-CIDS) enhances the precision of identifying malicious activity in cloud settings by using neural network learning capabilities together with the capability of fuzzy systems. The generation is specifically designed to uncover and analyze little patterns that support unwanted access attempts, hence fortifying security protocols for trustworthy cloud-hosted services. The conceptual foundation of FNN-CIDS is described in the study, along with how neural networks are used for pattern reputation and fuzzy common sense is covered for rule-based inference. The results of the trial clearly demonstrate the device's ability to identify different intrusion scenarios while minimizing false positives. This research provides a road map for strengthening cloud computing infrastructure dependability and developing robust security frameworks for cloud-based software applications. The goal of the research paper is to create an intrusion detection system that guarantees there is no unwanted access to cloud services and a trust assessment machine that rates the dependability of cloud services. The self-building clustering algorithm used in the construction of the cloud intrusion detection system is mainly based on neuro-fuzzy techniques This method's overall performance in cloud intrusion detection has been compared with other well-established clustering algorithms using end-to-end assessment.

Keywords: computing, security, strengthening, algorithm

1. INTRODUCTION

Cloud computing is a platform that enables easy and widespread access to a shared pool of interconnected resources, available whenever needed. It enables corporations, organizations and individuals can avail services without incurring infrastructure expenditures or maintenance obligations.Because of this easiness, they can focus on growing their business without worrying about the infrastructure's manageability. Cloud storage solutions provide users many ways to organize and manage their data. However, these technologies provide a means of reducing security threats. These dangers could potentially exist. The course covers two aspects: the risky scenarios that cloud service providers face while providing services to cloud buyers, and the safety difficulties that cloud customers have when using cloud provider carriers' products.Users no longer have physical access to the website hosting server when they entrust the carriers with their sensitive data. Providers use a variety of strategies to guarantee the delivery of relaxed products in order to satisfy their customers' safety criteria. However, security concerns persist.An effective security monitoring system should possess the ability to intelligently detect security vulnerabilities and promptly respond to them by implementing any of the following approaches[1]:Deterrent or preventive mode refers to a strategy or approach aimed at deterring or preventing something from happening. Through the use of robust authentication measures, access to resources is restricted exclusively to authorized users. Access is restricted to authorized users, and administrators are alerted about any unauthorized attempts.

Mode of operation for a detective

Through the monitoring of user behavior on systems and networks, the security system may distinguish between conventional and abnormal attempts to gain access.Using this data, the system will identify harmful actions and notify the administrator. Remedial Mode Aside from identifying malicious behaviors, this system also engages in various restorative tasks. Restoring a system that has been compromised.

Incursion and Systems for Detecting Incursions

Intrusion refers to any unauthorized attempt to access cloud resources. Multiple intrusion detection systems and various methods are available to detect and pinpoint such unlawful activities. An intrusion detection system (IDS) can activate alarms using two primary triggering mechanisms:.identification of anomalies and misuse. An Intrusion Detection System (IDS) that is based on abuse detection uses a preset set of rules that may be manually written by the administrator or automatically produced by the system. It performs real-time monitoring of network and system processes, namely analyzing packets. It employs a rule-based approach to detect and identify attacks by searching for recognized signatures One benefit of this method is that, with the help of modern technology, signatures can be quickly and easily made and recognized once community behavior is known.This system necessitates a signature for every attack and solely identifies familiar attacks that are rooted in unchanging behavioral patterns. In order to attain the highest possible true positive rate, it is crucial to continuously revise the set of rules. Therefore, it is necessary to add new signatures to the Intrusion Detection System (IDS) whenever they are needed. This will result in an expansion of the rule set, thereby leading to an increase in resource use.Utilizing anomaly detection techniques Intrusion Detection System (IDS) is a surveillance system that may identify unauthorized access attempts by monitoring and categorizing system actions as either typical or abnormal, using predetermined metrics or regulations. An attack is defined as any activity that deviates from the regular category. To effectively mitigate attack traffic, the system needs to be trained to recognize and understand typical system behavior. This can be achieved through various methods, typically utilizing soft computing techniques.A mathematical model is used to precisely describe the machine's usual use sample in the context of strict anomaly detection. For a system of this kind to accurately reflect customary use patterns, it needs a profile of the machine or network. Accurate identification of this strategy requires a thorough understanding of typical network dynamics.After defining the behavior, the IDS may be readily expanded.

This method surpasses the abuse detection-based technique. Intrusion Detection Systems (IDS) have the capability to identify and detect novel assaults that do not have predefined signatures, as long as these attempts deviate from usual usage patterns. Nevertheless, it is susceptible to the drawback that malevolent behavior that conforms to typical usage patterns could go unnoticed, leading to the occurrence of inaccurate errors. Furthermore, alongside the implementation of a triggering mechanism, there may be monitoring of invasive behavior at designated locations within the network. There are two prevalent methods of monitoring.

Locations relate to the two types of intrusion detection systems: community-based and host-based. An entirely network-based intrusion detection system is made to recognize and show any unwanted actions carried out by users on the host or operating system platform. Through the analysis of machine calls, device and application log files, unusual changes to the report device, community assaults directed at the specific machine, verified signature attacks, port scans, and backdoor searches, the device finds intrusions. It has advantageous due to its convenient ability to determine the outcome of an attack, whether it is successful or unsuccessful. However, it has the challenge of accurately depicting a network or effectively controlling the activities occurring throughout the entire network.Additionally, it must becompatible with several operating systems in order to execute on all monitored hosts.A network-based intrusion detection system searches network traffic for signs of malicious activity in an effort to find instances of unwanted access to a computer network. One way to determine if a packet is malicious is to compare it to a database of known attack signatures or use aberrant packet behavior that indicates malicious activity to identify the malicious nature of the packet. It is not necessary for this device to perform effectively with every operating system that is used on a network. However, as networks become longer, a community-based Intrusion Detection System (IDS) placed in a single-family neighborhood may not be able to successfully gather all of the community's visitors. Consequently, a substantial quantity of sensors is necessary within the network, resulting in an elevated expense for the Intrusion Detection System (IDS).By combining some of the previously discussed intrusion detection techniques, a hybrid intrusion detection device may be produced. Many of this device's shortcomings may be efficiently overcome by using a variety of improvement tactics. However, because to the varying operational mechanisms of different IDS technologies, integrating them into a unified system is an exceedingly complex undertaking.Based on its organizational structure, IDS is divided into three categories:

dispersed, hierarchical, and centralized. In a centralized system, data gathered from one or more hosts is sent to an appropriate area for analysis, where a primary unit node is responsible for detecting malicious activity. An inherent limitation is that any malfunction in the central unit results in the deactivation of the intrusion detection system.Additionally, it must efficiently handle large amounts of data obtained from several hosts.The network is divided into a series of hierarchical clusters, with cluster chiefs responsible for identifying intrusions. Alerts from cluster-heads at the lowest degree are sent to heads at the next higher degree by heads at the higher degree, who take into account alerts from both the lower and their own level.While this strategy is more extensible than the centralized model, the critical unit continues to act as a bottleneck. Extra scalability is made possible by the distributed design that allows each server to run an intrusion detection system without the need for a central coordinator. However, at some stage in the decision-making process, the availability of full alert data may be restricted, leading to a reduction in accuracy.

Motivation

Even while cloud computing offers many benefits and conveniences, there are some drawbacks that make some consumers hesitant to put their confidence in it. Cloud forensics issues, loss of physical control, liability between two parties, adherence to privacy policies, backup plans, disaster recovery, multi-tenancy issues, security of hypervisors and operational structures, decision-making regarding data ownership and updating, and privacy issues are just a few of the difficult scenarios that the device must handle. All of these difficulties are centered around a single common factor known as 'cloud security', which can be categorized into two types:

1. Physical security refers to measures taken to safeguard against natural disasters andrisks.
2. Internet security refers to the measures taken to safeguard against deliberate attacks that can arise through the interconnectedness of computer networks.

Cloud systems are susceptible to intrusions due to their inherent openness. Intrusion refers to the deliberate attempt by unauthorized individuals or entities to obtain unauthorized access to cloud resources. Cloud security is constantly questioned. As a result, numerous studies are being conducted in the subject of cloud security with the aim of achieving access without any unauthorized intervention. However, the development of a cloud intrusion detection system (CIDS) that produces accurate results in terms of aid use, scalability, rapidity, and detection accuracy is still ongoing. Because of the dynamic behavior of both consumers and service providers, cloud safety has garnered significant attention in study. Through a comprehensive analysis of current intrusion detection systems, it has been discovered that while each solution reaches a certain level of accuracy, they often fall short in other crucial aspects. Therefore, the objective is to create a highly effective cloud intrusion detection system in order to ensure cloud security.Typically, customers of cloud services (CSCs) must evaluate the reliability and credibility of cloud service providers (CSPs). Due to the possibility of malevolent intent on the part of service providers themselves. Because of the potential for insider attacks, this distrust has grown. In the same way, cloud service providers try to determine the dependability and credibility of the individuals or organizations who use their services. Having access to this information will enable service providers to refuse subscriptions to questionable clients, hence streamlining their intrusion detection process.Therefore, it is essential for service customers and service providers to have a mutual trust in order to guarantee the seamless supply and utilization of cloud based services.

2. RELATED WORKS

Because of its ease and flexibility, cloud computing is attractive to a lot of individuals and organizations. However, there are a number of barriers that prevent certain consumers from using particular cloud services. Of all the difficult circumstances, protection is the one that affects people the most. For the most part, clients keep tool identification statistics, behavior facts, sensitive facts, and personally identifiable information in the cloud [2].Despite the efforts of several academics to develop various security-related solutions, the issue of security remains a pressing dilemma..The security, privacy, and reliability of cloud computing are the subjects of ongoing research projects that are presented in this phase. In addition to focusing on intrusions, the analysis often looks at the primary barriers to the growth and acceptance of cloud computing and investigates novel methods for trust evaluation and intrusion detection.The utilization of open and virtualized resources in cloud computing gives rise to security controversies, which encompass the following:

1. Concerns about privacy that come with using a multi-tenant design.
2. Loss of control over customers' sources and personal information
3. Increased likelihood of security breaches

Instructional and commercial researchers have suggested a number of cloud safety approaches.Cloud

service providers mustuse a proper combination of one or more security mechanisms in order to gain the trust of individuals and businesses. This trust is crucial for enhancing their corporate reputation[3].
Researchers have extensively discussed several aspects of cloud security. The hazards associated with cloud computing can be classified into three main categories [4]: security risks, privacy concerns, and consumer risks. Implementing measures to prevent a system from being targeted by a variety of assaults will result in a system that is secure. Data integrity, availability, records accessibility, records proximity, and network load are the main factors that might jeopardize cloud security.Privacy refers to the act of ensuring the confidentiality of consumers' data.Some consumers may be unwilling to share their data with others. However, data kept in cloud systems are susceptible to security breaches.. Rather, vulnerabilities within the privacy regulations specified in provider level agreements may potentially be introduced by cloud carrier suppliers themselves. Furthermore, it's possible that cloud service providers may alter the terms and conditions of their offering. Consumer concerns might arise when individuals are ignorant of these adjustments, thereby compromising their security and privacy. Therefore, it is important for customers to be knowledgeable about the terms and circumstances as well as the solutions provided by CSPs to guarantee privacy.

Cloud security

Despite the presence of a secure and trustworthy cloud infrastructure, both internal and external threats continue to occur.Cloud service providers have the potential to harm consumers' data, whether it is done intentionally or unintentionally. Any anyone with physical access to thecloud server has the ability to inflict harm on users' data. Due to the lack of preserved copies of their data, consumers face challenges in verifying the integrity of their outsourced data. A methodology based on Unified Modeling Language (UML) has been proposed to address the security issues in cloud models [5].Encryption and access control techniques are often used to guarantee user privacy. When data is encrypted using a few keys in cloud settings, access control-based techniques may be used to ensure privacy.However, a drawback of this method is that users must be provided with keys throughout the registration process. This issue, in turn, presents challenges in preserving the confidentiality of keys as consumers navigate between various cloud services. Researchers have devised many techniques to ensure the privacy of users in cloud storage [6]These solutions, however, call for the employment of compound encryptions, which might be inefficient in terms of the usage of valuable resources. Additionally, they have complexities in managing the addition and deletion of customers inside the cloud environment. Unique security approaches seek to preserve Parallel Distributed Processing (PDP) assets, which ensures the accuracy of data stored on cloud servers for users [7]. Nevertheless, their responses fall short of meeting a number of crucial security requirements, including public verifiability, dynamics, scalability, privateness, and authentication. As a result,[8]we used a cooperative Parallel Distributed Processing (PDP) approach that often targets two types of attacks: tag forgery and data leakage. Furthermore, it has been said that all statistics integrity testing methods should be inexpensive and easy to use in terms of computation and communication. However, this strategy yet involves a small amount of additional cost in terms of transmission and computing.

Cloud intrusion

Clients using cloud services who are legal make an effort to get access to unapprovedoffers. Specifically, individuals with privileged access to cloud systems will engage in deceitful actions and pose significant risks to security in various aspects. Studies indicate that these kind of attacks must be addressed with utmost seriousness.

Flooding attacks

Initially, intruders will gain access to one of the authorized hosts. Upon gaining access to the host, the intruders initiate the transmission of a substantial volume of packets. Engaging in such behaviors will result in Denial of Service (DoS) attacksknown as Denial of Service(DoS). A single server will not be able to provide the expected services due to direct assaults. In addition, side assaults affect more than just the targeted webpage.They disrupt interconnected services that rely on the affected server, rendering them inaccessible to users.[9][10]. Unauthorized access attempts by users to gain root-level privileges. Intruders employ various methods such as password-guessing tactics, keyloggers, or phishing mechanisms to illicitly access the accounts of legitimate consumers. Thus, gaining root-level access to virtual machines or structures is their ultimate objective.

Scanning sports

Attackers routinely test several ports in order to get information such as IP addresses, physical locations, and specifics about firewalls, routers, and gateways. Afterwards, they find open ports that allow certain services to be accessed and used for illicit activities.

Covert Communication Channel Exploitation

Intruders exploit disrupted resources as a base for executing Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Because these assaults just involve port scanning, they are regarded as quiet.However, it raises concerns about the confidentiality obligations of genuine consumers. [11] proposes a cloud intrusion detection system that relies on audits..Similar strategies exist, however they don't address middleware vulnerabilities, high-level data vulnerabilities, or attacks that target specific cloud infrastructure. Every node has an intrusion detection system installed, and these devices work together with other nodes to identify intrusions. Every customer's behavior is verified by the conduct analyzer, which compares it to that of a typical client. By using a knowledgebase with details on previous attacks, the expertise analyzer detects assaults. An artificial neural network that uses three different types of behavioral records—lawful activities, malicious moves, and policy violations—is used in the studies. However, the findings are not examined in terms of the accuracy, speed, and scalability of identifying every kind of attack throughout the training and testing stages.Furthermore, this approach requires a substantial amount of training data.Previous studies [12][13][14]have proposed practical approaches for detecting and preventing intrusions in cloud computing. These approaches involve the use of. risk management, fuzzy judgment, ontology, and autonomic computing.

The report outlines many essential attributes that an effective cloud intrusion detection system shouldpossess:1. Should be able to operate in a very dynamic, real-time environment with minimal or no human interaction.

2. The system should possess the ability to attain optimum accuracy in identifying new forms of attacks that may occur in the future. This means that the system should be capable of self-learning.

3.The time required for intrusion detection should be minimized to ensure early detection and prevent potential harm.

4. The inclusion of self-configuration competency is necessary to effectively handle configuration changes in a cloud computing environment.

5. It is important for the system to be dependable and provide a reasonable level of services, even in the face of failures, while minimizing the amount of processing and communication required.

6. Must have the capability to collaborate with other intrusion detection systems that are running simultaneously in a distributed setting.

7. Must has the capability to defend oneself.

8. Should be adaptable to evolving user behavior, system dynamics, and network conditions.

It is highly recommended that traditional intrusion detection systems (IDS) be replaced with cloud-based intrusion detection systems (IDDS) after a comparison of their characteristics and requirements was made.A study conducted by [15]has established an intrusion detection model that utilizes threads, taking into account the distinctions between these two forms of intrusion detection systems. Regrettably, this strategy requires extra resources for managing thread scheduling and is deficient in identifying attacks originating from the host.An alternate method that gives each user a personalized intrusion detection device has been suggested. These character IDSs are synchronized using an impartial controlled. This method mostly relies on detection that is based on signatures. Moreover, it investigates the process of recognizing unusual assaults as well as the exhaustion of other sources. Using a SaaS transmission mechanism, a comparable method has been devised with the assistance of [16]that solves the limitations of traditional IDS. A centralized detection controller and a group of lightweight intrusion detection system (IDS) sellers are integrated into the network. Yet, a network reporting massive visits should not use this technique.Therefore, the expense associated with communication and computation will be significant. In [17], it was suggested to implement an Intrusion Detection System (IDS) by installing individual IDSs in each virtual machine.. In order to facilitate collaboration between them, a cloud alliance concept has been developed that leverages behavior-based intrusion detection strategies and integrated knowledge. This method may effectively identify malevolent sports even in the event of single-point errors. In [18], the authors put out a methodology that combines intrusion prevention and detection features into a cloud model. Despite using both integrated anomaly and signature-based detection, their version of the method lacks experimental support for its efficacy. A similar CIDPS has been constructed by [17]and it has also been described solely from a theoretical perspective.A comprehensive analysis of several cloud security concerns has been published in reference [18]Backdoor and debug alternatives, CAPTCHA breaking attacks, cookie poisoning, move-website scripting attacks, denial of service (DoS) attacks, dictionary attacks, hidden disciplinemanipulation, guy-in-the-middle attacks, and square injection attacks are the main threats to information and application security. The issue of reusing IP addresses, DNS attacks, sniffer attacks, and BGP prefix hijacking may all jeopardize community security. A review of many security protocols pertaining to storage security, user privacy, cloud trust, and virtualization has been conducted, taking those types of attacks into account. The advantages and disadvantages of such plans had been thought out. The authors came to the conclusion that a security system should be able to protect data from all potential threats. According to [19], a virtualization-based intrusion prevention system effectively counteracts certain network-based attacks. This version is housed within a digital machine, and its function is to monitor packet flow in order to identify and detect any attempts at unlawful get-right entrance.This method, in which the state-of-the-art status and transition of each digital device are represented using deterministic finite automata (DFA), is intended to explain the constantly changing properties of clouds.However, this approach results in increased computing complexity when there is a significant amount of network traffic.The user behavior-based Cyber Intrusion Detection and Prevention System (CIDPS) was developed in [20]. Using this method, a fantastic profile is created for each user on each digital device. This profile is generated by the examination of past client movements and the acquisition of control of virtual computers at arbitrary times. Next, the detection module looks at network site visits that go across computers.The utilization of the saved profile, and the profile database is compared to the visitors' typical behavior. The comparison's results indicate whether or not there have been any intrusions.To ensure that new risks are identified, the profile database is regularly updated.However, on occasion, this method is ineffective in identifying impersonation attempts.This project aims to expand and investigate the capabilities of cloud intrusion detection systems that employ statistical analysis in conjunction with a fuzzy self-constructing clustering set of rules. The research project aims to achieve the following main goals:

1. The objective is to develop an intrusion detection system that can detect malicious users whose actions jeopardize the security and privacy of authorized cloud users and theirassets.
2. to use mean square errors as the only criterion for evaluating the intentional system's performance.
3. to assess how well the machine performsin comparison to other clustering techniques.
4. To get the highest level of accuracy in identifying intrusions.

3. The Suggested Approach

This section discusses how to create a cloud intrusion detection system using a self-constructing clustering technique that is entirely based on neuro-fuzzy.Statistical analysis is done in the field of cloud intrusion detection [21]to compare the overall effectiveness of this method to that of other clustering techniques. This study advances the fuzzy Neural network assisted cloud intrusion detection system (FNN-CIDS) for an Infrastructure-as-a-service (IaaS) paradigm. As shown in figure 1, this device is constructed as a hybrid device that combines fuzzy structures and artificial neural networks (ANNs).

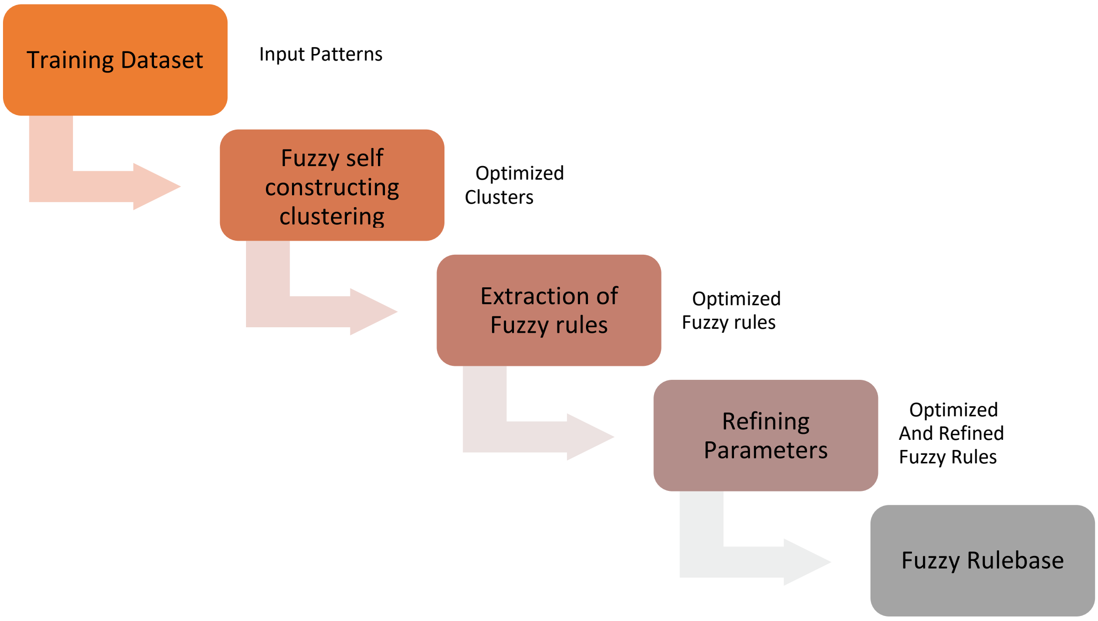


Fig 1. Architecture of a Cloud Intrusion Detection System Enhanced with Fuzzy Neural Network

This system is comprised of three distinct steps, namely:
Stage 1: Cluster formation
Stage 2: Removing ambiguous policies
The process of refining and enhancing the antecedent and consequent factors is covered in stage 3.

Fuzzy Neural Community Algorithm:

The algorithm used by the Assisted Cloud Intrusion Detection Device (FNN-CIDS) is a methodical process or collection of instructions for resolving a specific issue or completing a specific task.

Begin {algorithm}

Obtain the main input pattern in step one.

Step 2: Determine how similar each contemporary cluster is to the modern pattern.
Step 3: Determine the output similarity between the cutting-edge pattern and each of the existing clusters if the cutting-edge pattern satisfies the requirements for input similarity.

connect the current sample with the appropriate cluster if the current pattern satisfies the output similarity criteria. If only one cluster passes both tests, then connect the current pattern with that cluster.

Update its club feature

If several clusters satisfy both requirements

Next

Choose the cluster with the most advanced membership diploma.

Label it as a hit cluster.

Connect the successful cluster to the current pattern.

Adjust the success cluster's height, wide deviation, and average.

Equation (1) is used to determine the similarity between each pattern, Ii = [Ii1, Ii2,..., IiN], and each cluster, Cj. Here, mj is the mean of cluster Cj, and σj denotes the typical deviation of cluster Cj.[21]

$$\mu\left(\mathrm{I_i}, \mathrm{C_j}\right) \prod_{l=1}^{N} \exp\left\{-\left[\frac{\mathrm{I_{il}} - \mathrm{m_{jl}}}{\sigma_{\mathrm{jl}}}\right]^2\right\} \ldots\ldots(1)$$

The test for similarity between the present pattern Ii and cluster Cj is considered successful only if the requirement provided in Equation (2) is met.

$$\mu\left(\mathrm{I_i}, \mathrm{C_j}\right) \geq \omega_{\mathrm{in}}$$

The variable ωin is a predetermined input threshold that falls within the range of [0.0, 1.0]. The value of ωin influences the number of clusters..The number of clusters increases more when the cost of ωin approaches 1.0 increases. Each cluster in this context has a finite number of styles. Similarly, when the value of ωin approaches 0.0, the number of clusters diminishes. Each cluster in this instance contains a substantial quantity of patterns.A strict and quick input threshold, the variable ωin is restricted to the range of [0.0, 1.0]. A factor influencing the number of clusters is the cost of ωin. The number of clusters will also rise as the cost of ωin approaches zero. Within this particular environment, every cluster consists of a finite number of patterns.. Similarly, when the value of ωingets closer to zero, there are fewer clusters. Each cluster in this example has a vast range of styles that are used to illustrate the contemporary pattern. It is important to establish a new cluster called Cnew in this case.This cluster Cnew adheres to Equations 3 to 7 for the initialization of its parameters.

$m_{new} = [I_{i1}, I_{i2}, \dots \dots, I_{iN}] \dots \dots (3)$

$\sigma_{new} = \sigma_0 \dots \dots (4)$

$alt\, t_{new} = O_i \dots \dots\ (5)$

Where i is the sample as of right now, and σ 0 represents the preliminary deviation.

Alternately, the output similarity test is concluded if the enter similarity check for the dominant input sample is successful. A cluster's altitude (hj) is determined by computing the suggest of all the patterns' predicted outputs inside that cluster. The expression for 1 ≤ j ≤ $CC$is represented by equation (6).In this equation, the whole range of training styles that are a part of cluster j is represented by $PCNT$j, and the total number of clusters that are now present is indicated by CC.

$$alt_j = \frac{\sum_{l=1}^{PCN\,T_j} o_l}{PCNT_j} \dots \dots (6)$$

The difference between the height of each cluster Cj and the preferred output of the current pattern Ii is calculated using equation (7).

$diff_{ij} = |O_i - alt_j| \dots (7)$

In this context, the terms "$Oh$ig$h$" and "Olow" are employed to denote the upper and lower bounds of the desired output values correspondingly. Their difference is represented by $DIFF$, and it is ascertained by Equation (8). If Equation (9) is satisfied, pattern Ii is deemed to have passed the output similarity test for cluster Cj.

DIFF=|O_"high " -O_"low " |……(8)

$diff_{ij} \le \omega_{out}\ (DIFF) \dots . (9)$

where ωout is an output threshold that is predefined and is within the range out [0.0, 1.0]. To determine the divergence between the predicted and actual output, a threshold of |$Oh$ig$h$ − Olow| is established. For the current sample, there is very little chance of success in the output similarity test if the difference ($d$iffij) between the two outputs is beyond the range of $Oh$ig$h$ and Olow. In order to achieve a high level of accuracy, the parameters "Ohigh" and "Olow" provide a constraint on the output similarity check. The sample Ii is said to have passed the output similarity test if the condition given in Equation (9) is satisfied. The number and size of clusters are influenced not only by the input threshold ωin, but also by the output threshold ωout. As the magnitude of ωout increases, it results in a bigger value for the product (ωout. $DIFF$) in Equation (9).As a result, a large number of styles will effectively get through the output similarity check and be grouped together. The overall broad diversity of capability clusters may be lowered as a result. Since there are fewer clusters, each cluster must include every style in the detection dataset, which causes the cluster length to increase. The differences across clusters are impacted by this circumstance. Unfortunately, such gaps match styles for which there is no known output.In contrast, when the angular frequency lowers, the value of Equation (9), namely the product of angular frequency and Damping Induced Frequency Factor (ωout. $DIFF$), decreases. This complicates the evaluation of output similarity.Therefore, if the pattern closely approaches the dominant styles inside the equal cluster, it will pass this test the best. Consequently, the likelihood of cluster Cj passing the output similarity test with pattern Ii is reduced. Several additional clusters are created as a result of this circumstance. Consequently, the number of clusters will increase. Due to the fact that each cluster exclusively consists of highly similar patterns, the number of patterns within each cluster will be reduced. Consequently, the size of each cluster decreases. The gadget will display a greater abundance of tiny clusters as ωout decreases. The possibility of cluster overlap will rise along with the diversity of clusters. Ultimately, a pattern may be linked to a few clusters. Regarding the tests for resemblance between input and output, there are three specific cases:

Situation 1: Should the sample meet both requirements, it implies that the contemporary pattern could be associated with a cluster.

Situation 2: A new cluster will be introduced if the sample fails the input similarity test and the output similarity test is not completed for that pattern.Situation 3: Assuming that the input similarity test is surpassed , there is still a very slim chance that the pattern will fail the output similarity test. Conducting an output similarity test is still necessary for patterns that have passed the input similarity test. Additionally, during the parameter refining phase, this scenario leads to the development of premier clusters. When numerous clusters for the sample [Ii, Oi] satisfy the conditions given in Equations (1) and (9), the cluster with the best club diploma is designated as the winning cluster Cw. You may change the altitude, trendy deviation, and implication of Cw by using equations (10) through (13)

$$\mathrm{PCNT}_{\mathrm{w}}^{\mathrm{rev}} \,\&= \mathrm{PCNT}_{\mathrm{w}} + 1 \ldots\ldots (10)$$

$$m_w^{rev} = \frac{\sum_{l=1}^{PCNT_w^{rev}} I_{li}}{PCNT_w^{rev}} \;\ldots\ldots (11)$$

$$\sigma_{\mathrm{w}}^{\mathrm{rev}} = \sqrt{\frac{\sum_{\mathrm{l=1}}^{\mathrm{PCN\,T_w^{rev}}} (\mathrm{I_{li}} - \mathrm{m_w^{rev}})^2}{\mathrm{PCNT_w^{rev}} - 1} \ldots (12)}$$

$$\mathrm{alt}_{\mathrm{w}}^{\mathrm{rev}} = \frac{\sum_{\mathrm{l=1}}^{\mathrm{PCN\,T_w^{rev}}} \mathrm{o_l}}{\mathrm{PCNT_w^{rev}}} \ldots\ldots (13\ )$$

If an input pattern does not pass similarity tests, it indicates that the pattern cannot be represented using existing clusters. Therefore, it is necessary to establish a new cluster. This cluster's deviation will be 0 as it will benefit from having this input pattern from the beginning. It is not, however, suitable for use in evaluations of fuzzy similarity.The initial deviation is taken as $\sigma 0$. Subsequently, as novel patterns get linked to this cluster, its dimensions,

average, variation, and elevation are modified using Equations 10 to 13.

Similar to ωin and ωout, $\sigma 0$ also has an impact at the large range of clusters.When $\sigma 0$ is tiny, this clustering method only groups together patterns that are quite similar. This leads to the creation of a significant quantity of smaller clusters.Even if σzero is huge, a few styles may all be placed in the same cluster. Every cluster may also have a few outstanding styles that are connected to the deviation. This leads to the formation of a small number of bigger clusters.

4. RESULT AND ASSESSMENT

The efficacy of the suggested FNN-CIDS cloud intrusion detection device in identifying and identifying distinct attack types. Four different types of attacks—Denial of service (DoS), Probe, person to Root (U2R), and Root to local (R2L)—are supported by the KDD Cup 1999 dataset. The size of the cluster, the number of functions, and the percentage of school records utilized for instruction are taken into account when assessing the overall performance of the FNN-CIDS. The evaluation matrices that are used include F-rating, Accuracy, Precision, False Fantastic Price (FPR), and Technical PerformanceReport (TPR). Three alternative architectures are being used to assess the performance of the Adaptive Lion Neural Community cloud intrusion detection system: ok-means (Kulhare and Singh, 2013), FCM (Pandeeswari and Ganeshkumar, 2015), and WLI (Wu et al., 2015).

Denial of Carrier (DoS) Attack Detection

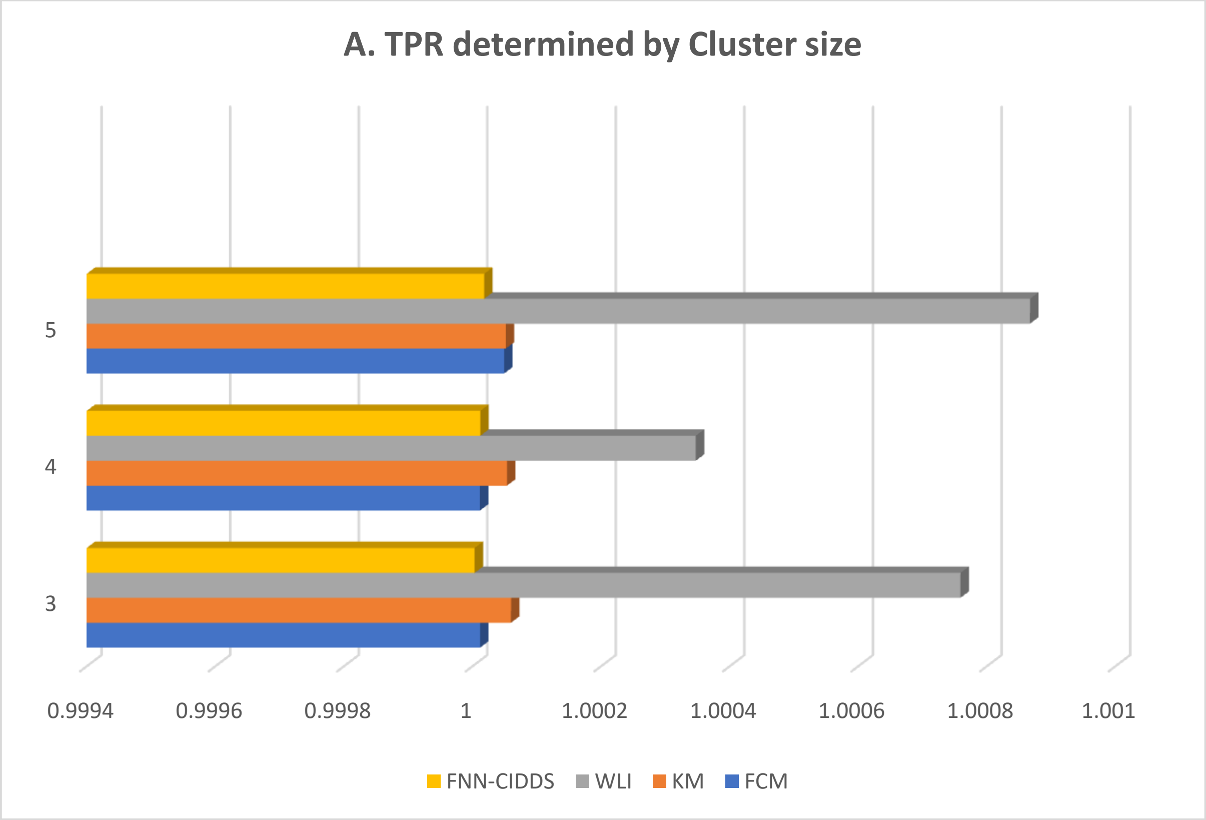
A denial of service (DoS) assault is launched by an attacker with the intention of preventing a legitimate target from being

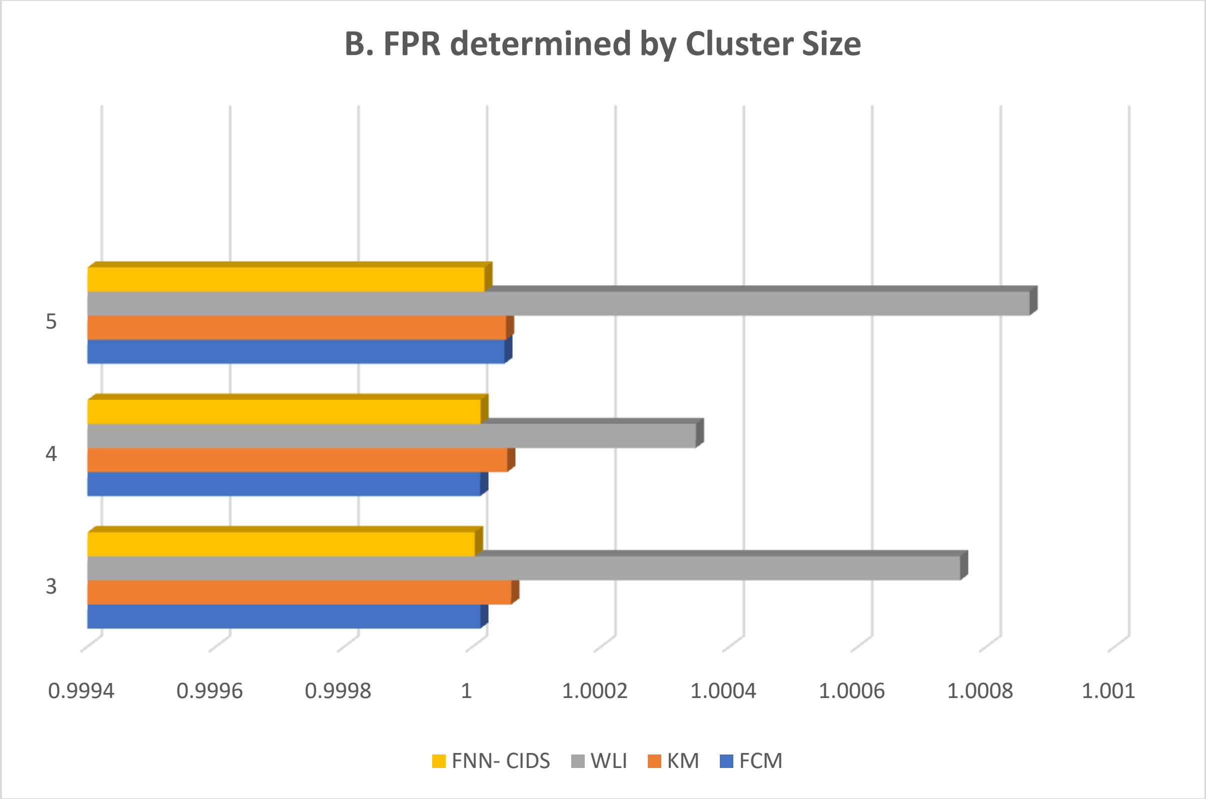
able to access authorized sources, so making them unavailable.Denial of Service (DoS) attacks account for as much as 80% of the overall attack landscape. Figure 1 and Table 1 display the outcomes achieved based on Cluster Size.

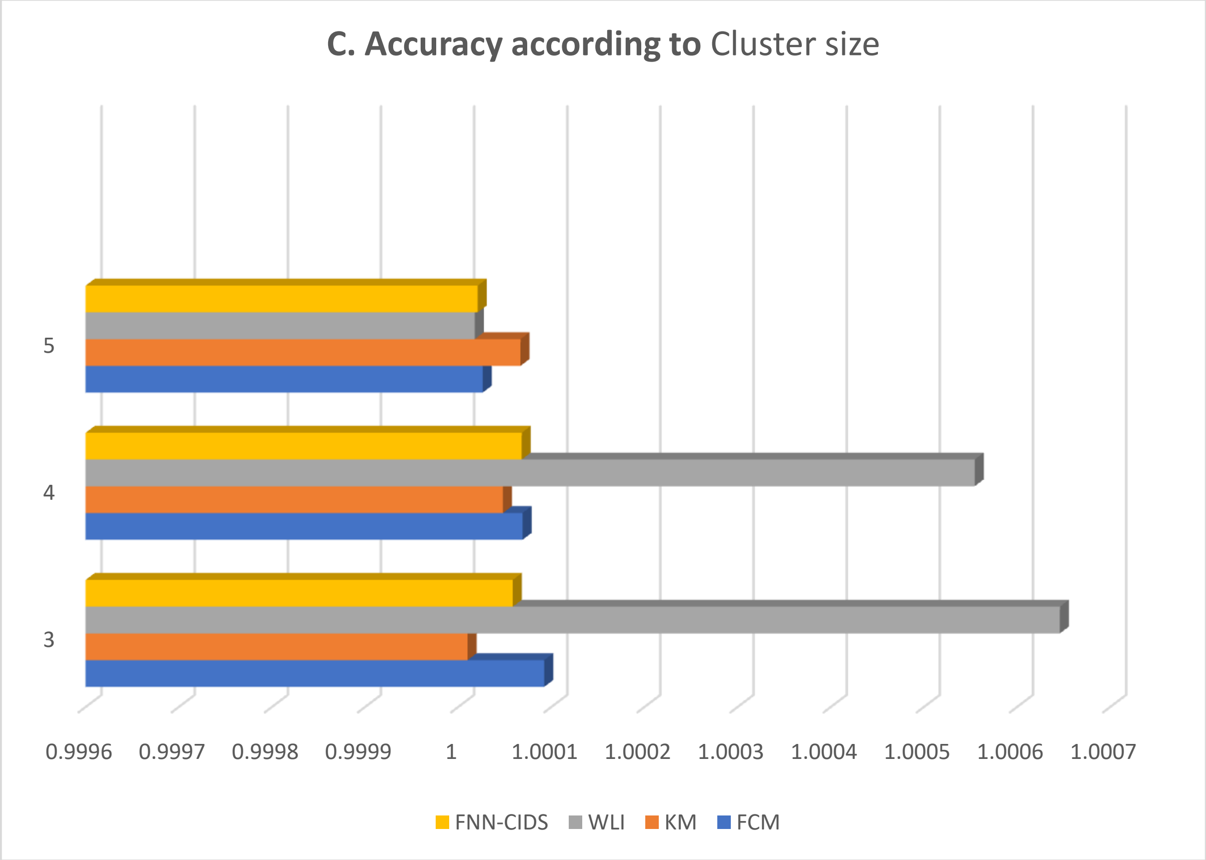
Table 1. Cluster size influences the performance of DoS attacks.

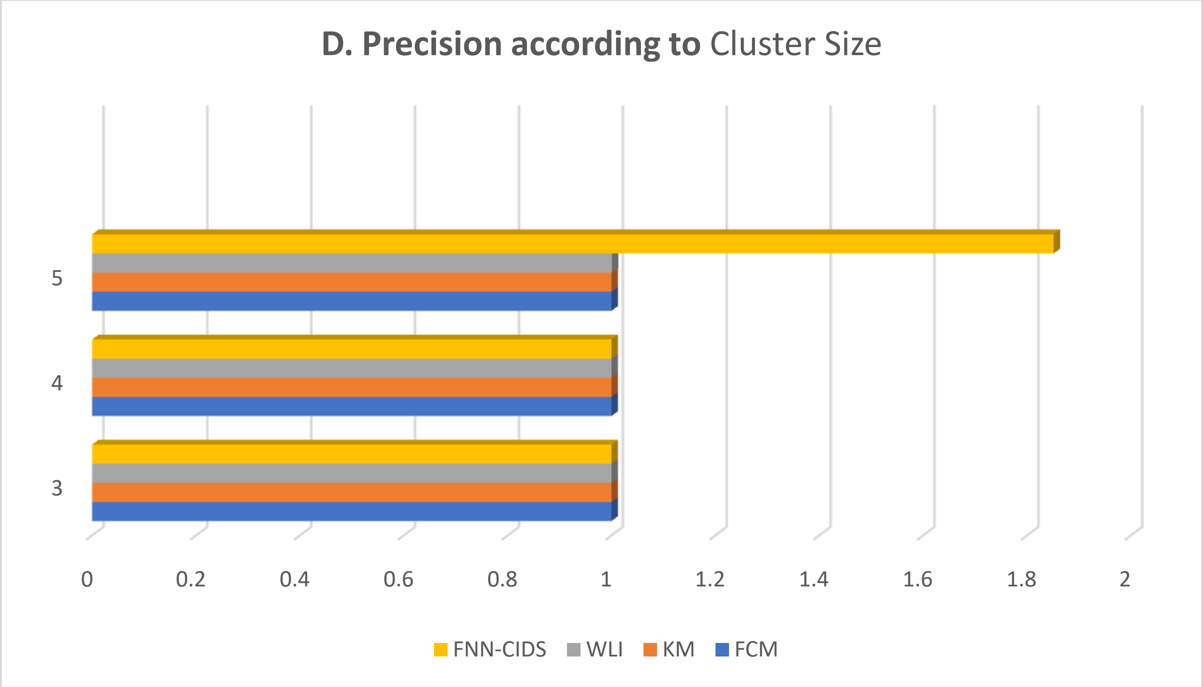
A. TPR determined by Cluster size				
Cluster Size	FCM	KM	WLI	posed FNN- CIDS
3	1.00001197	1.00006001	1.0007592	1.00000342
4	1.00001169	1.00005378	1.0003475	1.00001225
5	1.00004929	1.00005185	1.0008673	1.00001832
B. FPR determined by Cluster Size				
Cluster Size	FCM	KM	WLI	posed FNN- CIDS
3	1.00000023	1.00009866	1.0006929	1.00002997
4	1.00004086	1.00001927	1.0000776	1.00008276

5	1.00005406	1.00005904	1.0001538	1.00008276
C. Accuracy according to Cluster size				
Cluster Size	FCM	KM	WLI	posed FNN- CIDS
3	1.00009231	1.00000999	1.0006460	0005859
4	1.00006909	1.00004801	1.0005545	0006819
5	1.00002621	1.0000669	1.0000178	0002096
D. Precision according to Cluster Size				
Cluster Size	FCM	KM	WLI	posed FNN- CIDS
3	1.00002998	1.00006013	1.00000708	1.00007003
4	1.00005914	1.00008073	1.00002237	1.00001724
5	1.00004594	1.00004096	1.00084615	1.85140078
E. F-Score determined by Cluster Size				
Cluster Size	FCM	KM	WLI	posed FNN- CIDS
3	1.00056	1.000942	1.000093	1.00018
4	1.000683	1.000748	1.00209	1.000799
5	1.000986	1.000957	1.0047	1.000516

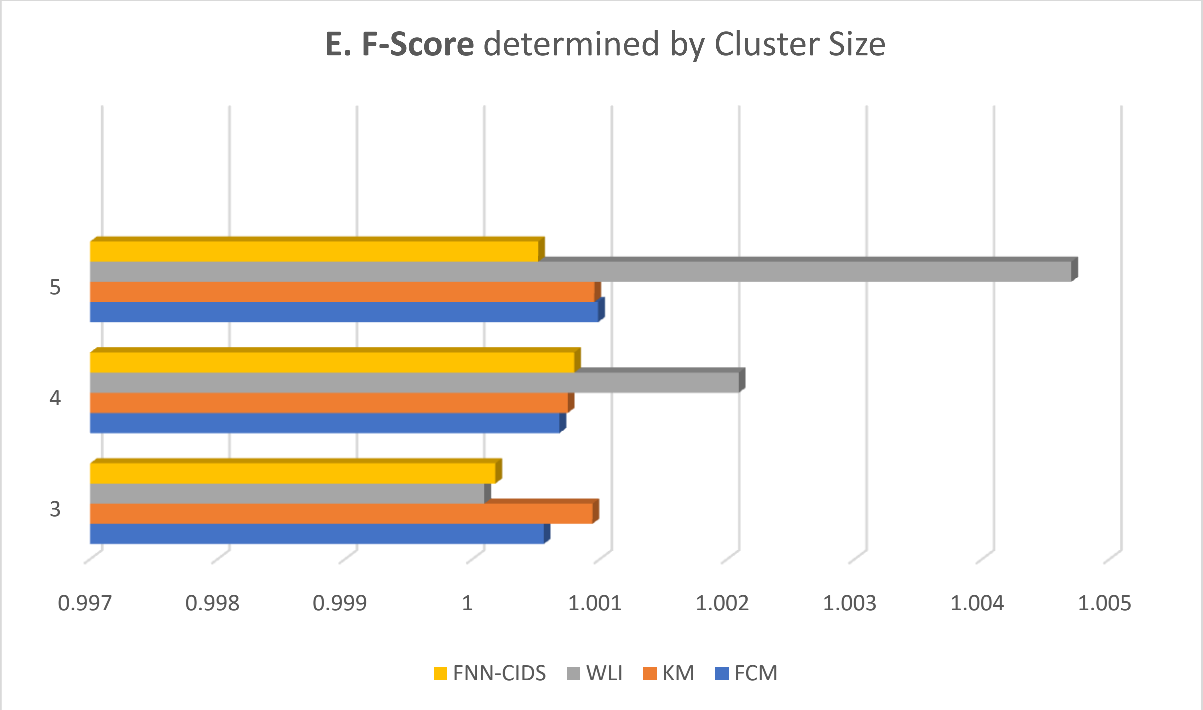



B. FPR determined by Cluster Size
5
4
3
0.9994
0.9996
0.9998
1
1.0002
1.0004
1.0006
1.0008
1.001
FNN- CIDS
WLI
KM
FCM


C. Accuracy according to Cluster size
5
4
3
0.9996
0.9997
0.9998
0.9999
1
1.0001
1.0002
1.0003
1.0004
1.0005
1.0006
1.0007
FNN-CIDS
WLI
KM
FCM



D. Precision according to Cluster Size



E. F-Score determined by Cluster Size

Figure 2(a) displays the True Positive Rate achieved by several algorithms. FCM achieves a rate of 90.33%, K-means achieves 90.8%, WLI achieves 92.7%, .additionally, FNN-CIDS attains an amazing rate of 92.7 percent.Based on Figure 2(a), it is clear that the suggested FNN-CIDS has the highest True Positive Rate. Figure 2(b) displays the False Positive Rate for several algorithms. The FCM algorithm has a rate of 26.3%, Kmeans has a rate of 22.9%, WLI has a rate of 24.6%, and FNNCIDS has a rate of 16.2%.. The recommended FNN-CIDS has the lowest false superb rate, as can be shown from Figure 2(b). Figure 2(c) displays the detection accuracy of different algorithms. FCM achieves an accuracy of 84.4%, K-means achieves 84.5%, WLI achieves.85.0%, whereas FNN-CIDS has a detection accuracy of 85.5%. Based on Figure 2(c), it is clear that the suggested FNN-CIDS achieves the best level of detection accuracy. Figure 2(d) displays the precision values achieved by several algorithms. FCM achieves a precisionof83.6%, okay-method 84.1%, WLI 85.38%, and FNN-CIDS 86.0% in terms of accuracy. It is evident from parent 2(d) that the warned FNN-CIDS achieves the highest level of accuracy. The F-score values obtained using unique techniques are shown in Figure 2(e). The F-scores for FCM, Okay-way, WLI, and FNN-CIDS are

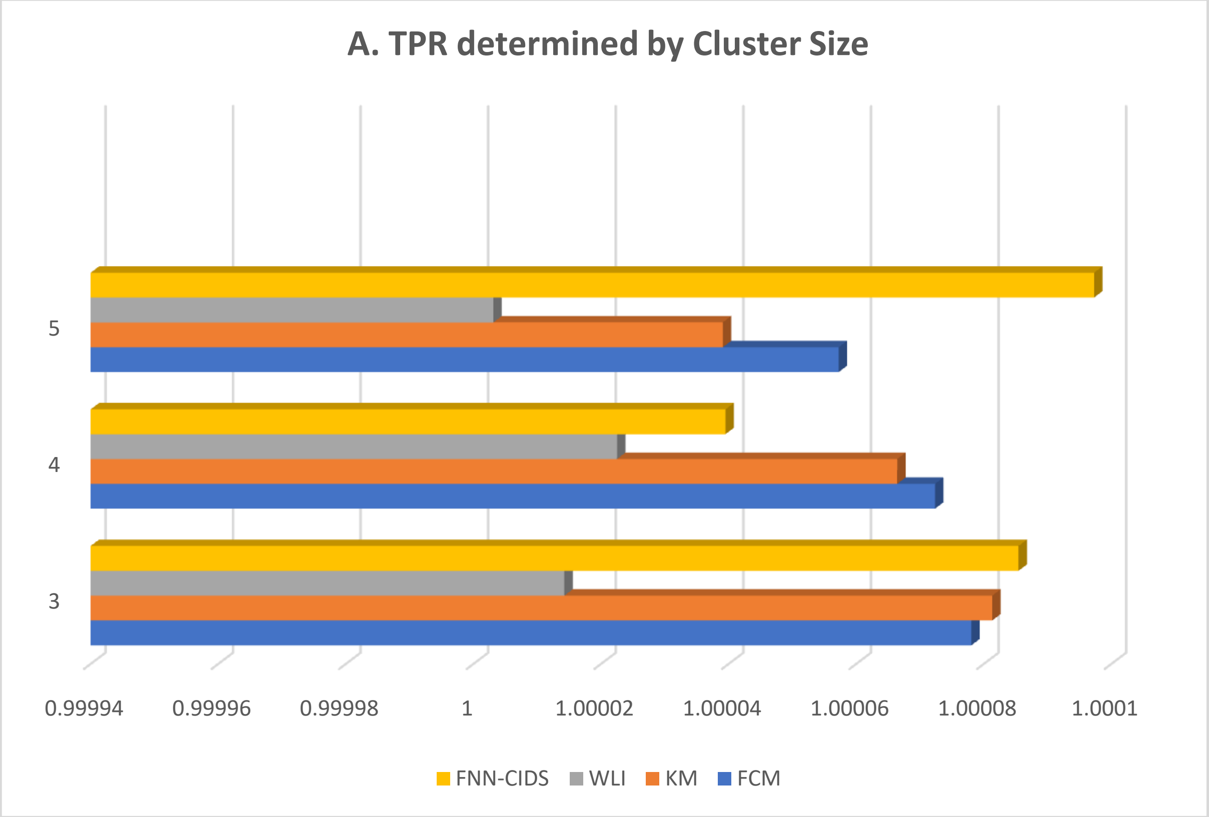
86.7%, 87.0%, 88.4%, and 89.3%, respectively. It is evident from figure 2(e) alone that the suggested FNN-CIDS obtains the highest F-rating cost.Based on the information provided in Figure 2 and Table 1, it can be concluded that the proposed FNN-CIDS is more effective in detecting Denial of Service (DoS) assaults compared to FCM, K-means, and WLI. The FNN-CIDS system has a true positive rate of 92.8% for detecting DoS assaults, a false-positive rate of 16.2%, an accuracy of 85.52%, a precision of 86.14%, and an F-score value of 89.35%. Furthermore, it is apparent that DoS assaults are not influenced by the quantity of clusters. When the cluster size is set to 3, DoS attacks exhibit the lowest rate of false positives.

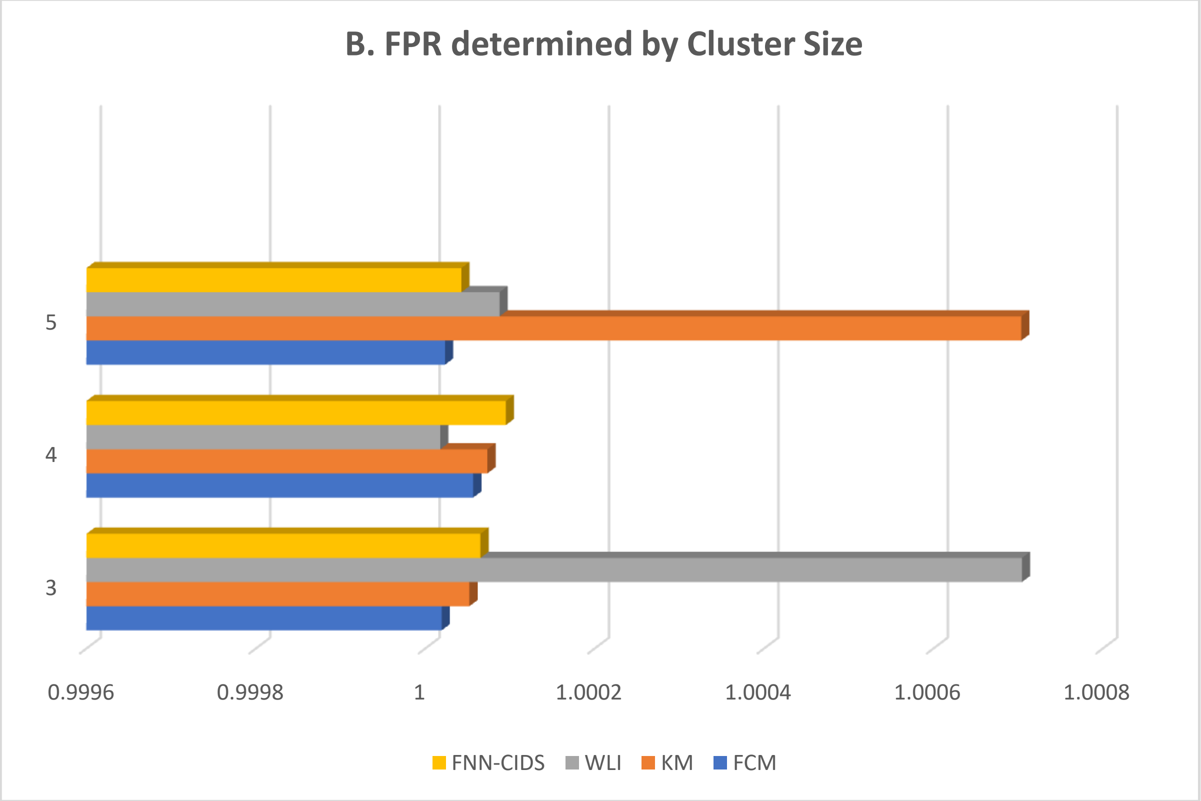
Identification of Probe Attack

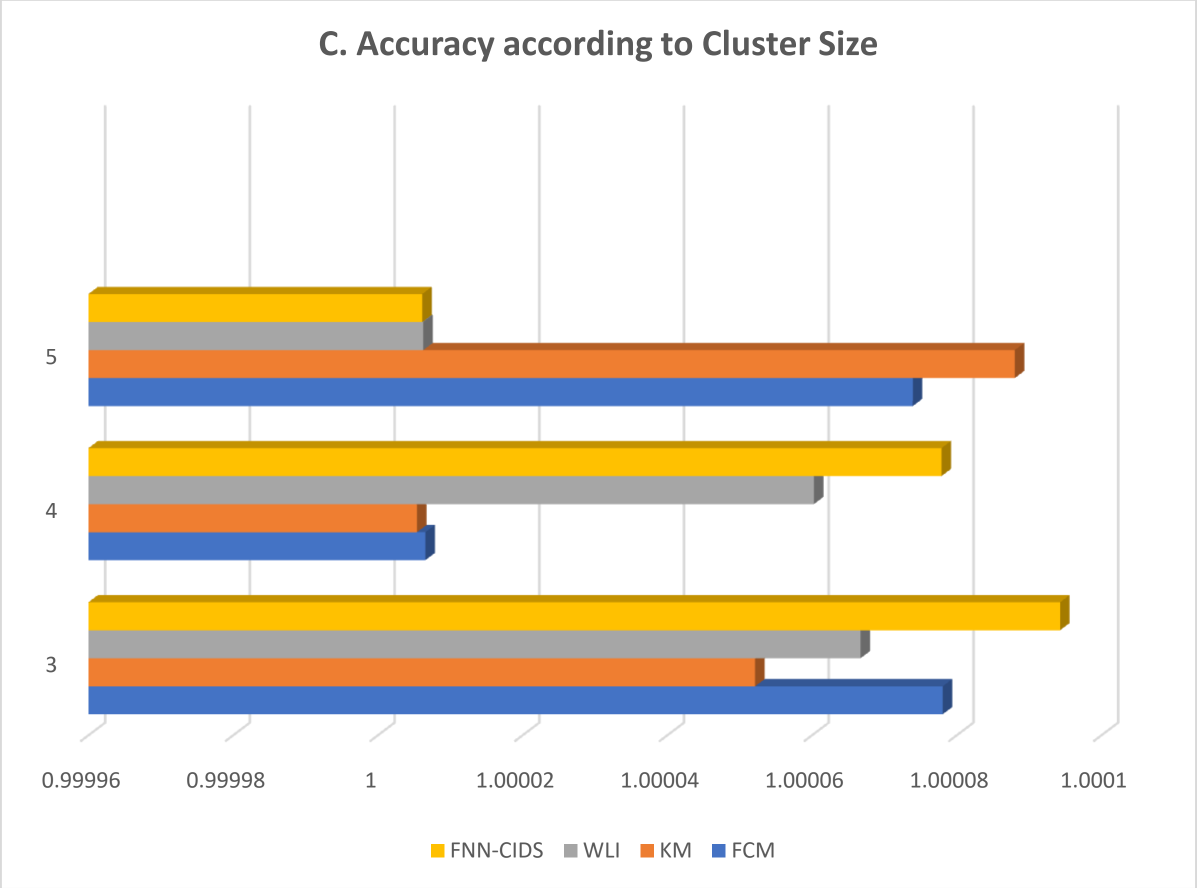
An intentional attack to perform port or host scanning in order to gather information or identify known vulnerabilities is known as a probe assault.About 1% of the overall attack space is occupied by probe assaults. The impacts obtained based only on the Cluster size are shown in Desk 2 and Distinguish 3.

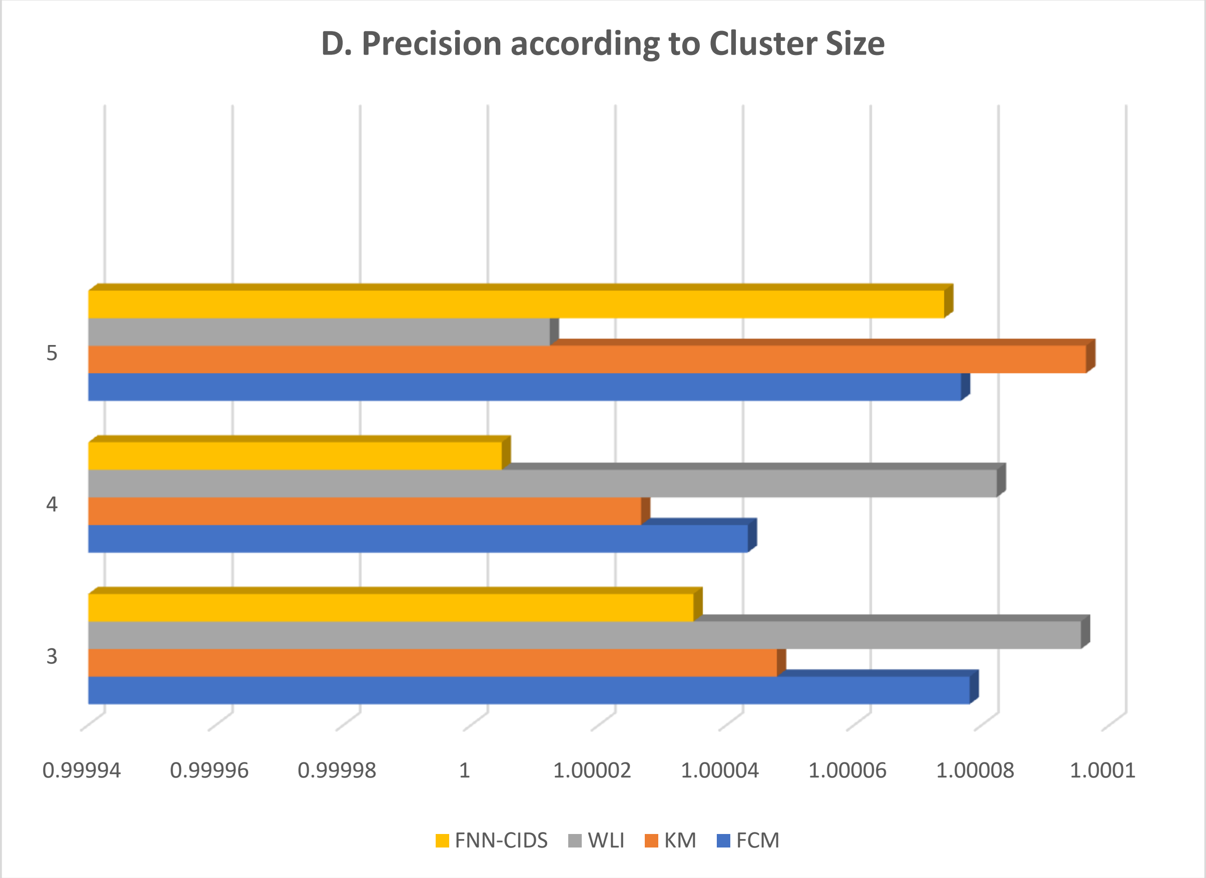
Table 2. Cluster size affects the performance of the probe attack.

A. TPR determined by Cluster Size				
Cluster Size	FCM	KM	WLI	proposed FNN-CIDS
3	1.00007806	1.00008133	1.00001425	1.00008545
4	1.00007236	1.00006643	1.00002251	1.00003951
5	1.00005726	1.00003909	1.00000313	1.00009729
B. FPR determined by Cluster Size				
Cluster	FCM	KM	WLI	Proposed FNN-
Size				CIDS
3	1.00001937	1.00005215	10007045	1.0000652
4	1.0000567	1.00007341	1.0000177	1.00009524
5	1.00002331	1.0007037	1.00008772	1.00004259
C. Accuracy according to Cluster Size				
Cluster Size	FCM	KM	WLI	Proposed FNN-CIDS
3	1.00007806	1.00005214	1.00006671	1.00009429
4	1.00000656	1.00000541	1.00006026	1.00007789
5	1.00007393	1.00008803	1.00000628	1.00000613
D. Precision according to Cluster Size				
Cluster Size	FCM	KM	WLI	Proposed FNN-CIDS
3	1.00007806	1.00004785	1.0000955	1.0000348
4	1.0000433	1.00002659	1.0000823	1.00000476
5	1.00007669	1.0000963	1.00001228	1.00007407
E. F-Score according to Cluster Size				
Cluster Size	FCM	KM	WLI	Proposed FNN-CIDS
3	1.00007806	1.000758	1.0094	1.000032
4	1.00007258	1.000144	1.000891	1.000267
5	1.00003075	1.000861	1.000971	1.000292


A. TPR determined by Cluster Size
5
4
3
0.99994
0.99996
0.99998
1
1.00002
1.00004
1.00006
1.00008
1.0001
FNN-CIDS
WLI
KM
FCM


B. FPR determined by Cluster Size
5
4
3
0.9996
0.9998
1
1.0002
1.0004
1.0006
1.0008
FNN-CIDS
WLI
KM
FCM


C. Accuracy according to Cluster Size
5
4
3
0.99996
0.99998
1
1.00002
1.00004
1.00006
1.00008
1.0001
FNN-CIDS
WLI
KM
FCM


D. Precision according to Cluster Size
5
4
3
0.99994
0.99996
0.99998
1
1.00002
1.00004
1.00006
1.00008
1.0001
FNN-CIDS
WLI
KM
FCM

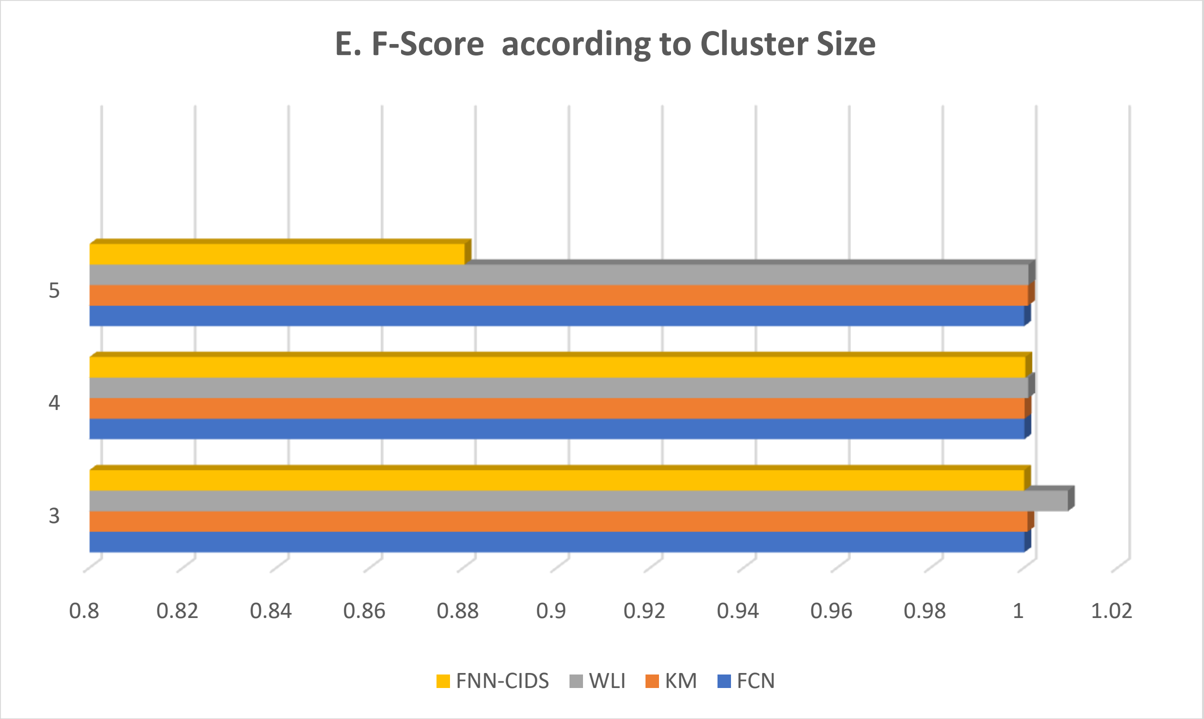


Figure 3 (a) displays the True Positive Rate achieved by several algorithms. Specifically, FCM achieves a rate of 80.24%, K-means achieves 80.56%, WLI achieves 80.89%, and FNN-CIDS achieves the highest rate of 85.45%. Based on Figure 3(a), it is clear that the suggested FNNCIDS has the highest True Positive Rate. Figure3(b) displays the False Positive Rate for different algorithms: FCM records a rate of 28.6%, K-means reports a rate of 27.87%, WLI records a rate of 23.50%, and FNN-CIDS records a rate of 21.13%. Based on Figure 3(b), it is clear that the suggested FNN-CIDS has the lowest False Positive Rate. Figure 3(c) displays thedetection accuracy of different algorithms. The FCM algorithm achieves an accuracy of 83.36%, Kmeans achieves 84.66%, WLI achieves 85.06%, and FNNCIDS achieves the highest accuracy of 87.38%. Based on Figure 3(c), it is clear that the suggested FNN-CIDS obtains the best level of detection accuracy. Figure 3(d) displays the Precision values achieved by several algorithms. FCM achieves a Precision of 81.32%, K-means achieves 82.12%, WLI achieves 83.9%, and FNN-CIDS achieves 88.65% Precision. Based on Figure 6.5(d), it is clear that the suggested FNN-CIDS has the highest Precision. Figure 3(e) displays the F-Score values achieved by different algorithms. FCM achieves an F-Score of 80.78%, K-means achieves 81.21%, WLI achieves 83.59%, and FNN-CIDS achieves 87.02%. Based on Figure 3(e), it is clear that the suggested FNN-CIDS gets the highest FScore value. Table 2 displays the data acquired for cluster sizes 3, 4, and 5, and presents a comparative examination of the detection of probe attacks based on cluster size.

5. SUMMARY

This study utilizes a fuzzy self-constructing clustering algorithm to integrate intrusion detection in a cloud environment. The algorithm is specifically applied to identify Denial of Service (DoS) and Probe assaults. The performance of the proposed CIDS and other approaches (FCM, K-Means, WLI) will be compared through a comparative analysis..Factors like the percentage of education records, the number of clusters, and the broad range of talents will all be taken into consideration during this examination. A series of testbed experiments utilizing the KDD dataset may be used to assess the effectiveness of such tactics. These actions have been taken to show the circumstances in which opportunity methods were outperformed by the hypervisor detection. This served as empirical evidence to support the justification of the hypervisor detector..It is admirable that FNN-CIDS is generally effective in identifying risky actions in the cloud environment.

REFERENCES

[1] A. Abraham and R. Jain, “Soft Computing Models for Network Intrusion Detec ct ti io on n S Sy ys st te em ms s.”

[2] S. Ahmad, B. Ahmad, M. Saqib, and R. M. Khattak, “Trust Model: Cloud’s Provider and Cloud’s User,” 2012.

[3] H. M. Alsafi, W. Mustafa Abduallah, H. Mohammed Alsafi, and A.-S. Khan Pathan, "IDPS: An Integrated Intrusion Handling Model for Cloud IDPS: An Integrated Intrusion Handling Model for Cloud Computing Environment." [Online]. Available: https://www.researchgate.net/publication/221703248

[4] A. Adhikari and P. Kulkarni, "Survey of techniques to detect common weaknesses in program binaries," Cyber Security and Applications, vol. 3, Dec. 2025, doi: 10.1016/j.csa.2024.100061.

[5] R. Ranjan, R. Buyya, R. N. Calheiros, R. Ranjan, and C. A. F. De Rose, "CloudSim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services," 2009. [Online]. Available: https://www.researchgate.net/publication/24164535

[6] J. H. Ang, K. C. Tan, and A. A. Mamun, "An evolutionary memetic algorithm for rule extraction," Expert Syst Appl, vol. 37, no. 2, pp. 1302–1315, Mar. 2010, doi: 10.1016/J.ESWA.2009.06.028.

[7] A. A. Sayed Aziz, M. A. Salama, A. ella Hassanien, and S. El-Ola Hanafi, "Artificial Immune System Inspired Intrusion Detection System Using Genetic Algorithm," 2012. [Online]. Available: www.egyptscience.netwww.egyptscience.net

[8] S. Iqbal et al., "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," Journal of Network and Computer Applications, vol. 74, pp. 98–120, Oct. 2016, doi: 10.1016/J.JNCA.2016.08.016.

[9] K. Balázs, L. T. Kóczy, and J. Botzheim, "Comparison of Fuzzy Rule-based Learning and Inference Systems."

[10] V. Bapuji, R. Naveen Kumar, A. Govardhan, and S. Sarma, "Soft Computing and Artificial Intelligence Techniques for Intrusion Detection System Network and Complex Systems Soft Computing and Artificial Intelligence Techniques for Intrusion Detection System," vol. 2, no. 4, 2012, [Online]. Available: www.iiste.org

[11] M. Khan et al., "Novel complex fuzzy distance measures with hesitance values and their applications in complex decision-making problems," Sci Rep, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-64112-6.

[12] R. Bhadauria, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques," 2012.

[13] B. Hui and K. L. Chiew, "An Improved Network Intrusion Detection Method Based On CNN-LSTM-SA," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 44, no. 1, pp. 225–238, Feb. 2025, doi: 10.37934/araset.44.1.225238.

[14] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. De Rose, and R. Buyya, "CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," Softw Pract Exp, vol. 41, no. 1, pp. 23–50, Jan. 2011, doi: 10.1002/spe.995.

[15] A. Adhikari and P. Kulkarni, "Survey of techniques to detect common weaknesses in program binaries," Cyber Security and Applications, vol. 3, p. 100061, Dec. 2025, doi: 10.1016/J.CSA.2024.100061.

[16] S. L. Chiu, "Fuzzy model identification based on cluster estimation," Journal of Intelligent and Fuzzy Systems, vol. 2, no. 3, pp. 267–278, 1994, doi: 10.3233/IFS-1994-2306.

[17] C. J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, "NICE: Network intrusion detection and countermeasure selection in virtual network systems," IEEE Trans Dependable Secure Comput, vol. 10, no. 4, pp. 198–211, 2013, doi: 10.1109/TDSC.2013.8.

[18] J. Cózar, L. De La Ossa, and J. A. Gámez, "Learning TSK-0 linguistic fuzzy rules by means of local search algorithms," Appl Soft Comput, vol. 21, pp. 57–71, Aug. 2014, doi: 10.1016/J.ASOC.2014.03.003.

[19] S N Dhage, "Intrusion Detection System in Cloud Computing Environment," 2011.

[20] S. Dolev, N. Gilboa, and M. Kopeetsky, "Efficient Private Multi-Party Computations of Trust in the Presence of Curious and Malicious Users Efficient Private Multi-Party Computations of Trust in the Presence of Curious and Malicious Users *," 2011.

[21] B. Archana et al., "International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Optimizing trust, Cloud Environments Fuzzy Neural Network, Intrusion Detection System." [Online]. Available: www.ijisae.org