applied sciences

MDPI

Article

Preventing the Cloud Networks through Semi-Supervised Clustering from Both Sides Attacks

Muhammad Nadeem [1], Ali Arshad [2,*], Saman Riaz [2], Syeda Wajiha Zahra [1], Ashit Kumar Dutta [3] and Sultan Almotairi [4]

[1] Department of Computing, Abasyn University, Islamabad 45710, Pakistan; nadeem72g@gmail.com (M.N.); syeda.wajia786@gmail.com (S.W.Z.)
[2] Department of Computer Science, National University of Technology, Islamabad 44000, Pakistan; samanriaz@hotmail.com
[3] Department of Computer Science and Information Systems, College of Applied Sciences, AlMaarefa University, Riyadh 13713, Saudi Arabia; adotta@mcst.edu.sa
[4] Department of Natural and Applied Sciences, Faculty of Community College, Majmaah University, Majmaah 11952, Saudi Arabia; almotairi@mu.edu.sa
* Correspondence: alli.arshad@gmail.com

Abstract: Cloud computing is a centralized data storage system providing various services worldwide. Different organizations are using the cloud for other purposes. As the number of users on the cloud server increases, so does the rate of attacks on the cloud. Various researchers have devised different solutions to solve these problems, the most widely used being the Intrusion Detection System (IDS). In this paper, a network architecture has been designed in which an efficient technique, semi-supervised clustering, has been used. In this technique, users' responses inside and outside the cloud server have been observed, and various rules and mechanisms have been enforced based on these responses. The network is divided into three different scenarios. In the first scenario, attacks outside the cloud server have been detected, and then ways to prevent these attacks are discussed. The second scenario uses Cloud Shell, allowing authentic users to access the cloud server through authentic queries. In the third scenario, this tool's performance and detection rate have been measured by applying different results to the confusion matrix. A comparative analysis has been done with other papers at the end of the paper, and conclusions have been drawn based on different results.

Keywords: intrusion detection system; cloud security; sids; semi-supervised clustering; network sensor; networking

Citation: Nadeem, M.; Arshad, A.; Riaz, S.; Zahra, S.W.; Dutta, A.K.; Almotairi, S. Preventing the Cloud Networks through Semi-Supervised Clustering from Both Sides Attacks. *Appl. Sci.* **2022**, *12*, 7701. https://doi.org/10.3390/app12157701

Academic Editors: Dimitris Mourtzis, Christos Bouras and Paula Fraga-Lamas

Received: 1 July 2022
Accepted: 28 July 2022
Published: 30 July 2022

1. Introduction

Cloud computing is a robust physical or virtual infrastructure that exists on various devices and servers and allows users to access online data instead of using an internal hard drive [1]. The concept of cloud computing is linked to distributed systems [2] because, even in a distributed system, the data are stored in different locations (servers). These data can be retrieved from any place where these servers are available. Cloud computing is a technology used to access data globally [3]. Cloud computing has four service deployment models: public, private, community, and hybrid [4]. A public cloud is a free cloud managed by a third party and provides free services to users. Amazon Web Service (AWS), Oracle Cloud, and Microsoft Azure are the most common public cloud providers. A private cloud is designed for a specific organization and accessible within that organization. The hybrid cloud is the third type of cloud computing, featuring the best features of public and private clouds. If an organization wants to use both public and private clouds, it uses the hybrid cloud. Community cloud is the fourth type of cloud computing. A set of organizations can access the systems and services through the community cloud. By 2021, the rate of cloud computing will remain something like this [5]:

- 73% of organizations turned to the private cloud;
- 92% of organizations turned to the public cloud;
- 69% of organizations turned to a hybrid cloud.

On average, 5 to 30 percent of companies have moved their organizations to the cloud [6]. Cloud computing has increased 2 to 3 times since 2013 and provides more than 1400 services [7]. The rapid advancement of internet technology has brought many conveniences in life, but security issues have increased rapidly [8,9]. According to the survey of 2021, the ratio of Ransomware malware attacks increased to 52.5 million [10], while Distributed Denial of Service (DDoS) attacks increased from 1392 per day to 2043 per day [11]. As the number of services in cloud computing increases, so does the number of attacks in the cloud. Different attackers have designed various algorithms to break cloud security and provide some algorithms to end-users in free applications. These applications can contain bugs and intrusions, allowing attackers to attack cloud servers quickly [12]. Many data centers have external security, while attacks on data centers are primarily from the inside [13]. This is because security mechanisms can detect external attacks and prevent data from being attacked, but internal side attacks can be challenging to detect. The growth rate of malware attacks is shown in Table 1.

Despite implementing various security mechanisms on the internal system of cloud computing, information leakage could not be prevented, and internal side attacks could not be reduced [14]. Network security is essential because the Internet is so widespread [15]. Many researchers have developed many algorithms that prevent cloud servers from attacks and designed a set of rules and policies that can be applied logically and physically to prevent the cloud from intrusions. So far, only a few solutions are available that are fully implemented on the cloud server [16].

Table 1. Growth rate of malware attacks.

SR#	*INTRUSION*	*GROWTH RATE*
1	Intrusion delivered by an email	92%
2	Increased malware attacks in mobile by applications	54%
3	Attacks by third-party application	99.99%
4	Increased Trojan Horse attacks in applications	45%
5	Increased attacks rate in Mac OS	16.5%
6	Malware development rate decrease in Windows OS	11.6%
7	Ransomware	70%
8	Backdoor	79%
9	Websites infected per week by malwares	18 million
10	Businesses affected by malware per week	34%
11	Financial Institute	90%

The growth rate of malware attacks increases by 20 to 30 times yearly [17], as shown in Figure 1. Overall, malware infections have been increasing over the last ten years.

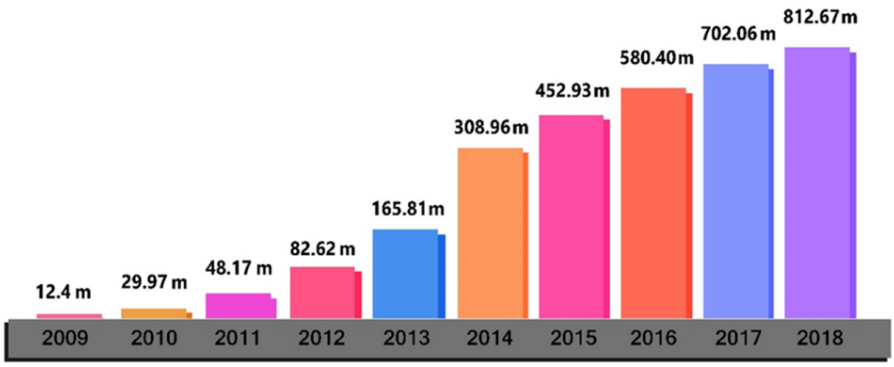

Figure 1. The ratio of malware from 2009 to 2018 (in millions).

- In 2009, the ratio of malware was 12.4 million;
- In 2010, the malware ratio increased from 12.4 million to 29.97 million;
- In 2011, the malware ratio increased from 29.97 million to 48.17 million;
- In 2012, the malware ratio increased from 48.17 million to 82.62 million;
- In 2013, the malware ratio increased from 82.62 million to 165.81 million;
- In 2014, the malware ratio increased from 165.81 million to 308.96 million;
- In 2015, the malware ratio increased from 308.96 million to 452.93 million;
- In 2016, the malware ratio increased from 452.93 million to 580.40 million;
- In 2017, the malware ratio increased from 580.40 million to 702.06 million;
- In 2018, the malware ratio increased from 702.06 million to 812.67 million.

Cloud security is needed to protect the cloud from intrusions and attacks. An intruder can never easily and quickly access cloud data but can try to access data without permission. To resolve this issue, firewalls were used on various Personal Computers (PCs) in the network. Firewalls have different rules and policies to protect the Cloud Personal Computers (PCs) from attacks. The network PC can prevent some intrusions, but firewalls alone are not enough to protect the network from intrusions [18].

The best way to protect the cloud from intrusions is an Intrusion Detection System [19]. An intrusion detection system is a technique that monitors all malicious activity on the network and protects the cloud from all such activity [20]. IDS has attracted many researchers. An IDS can protect all networks and their components [21]. When cloud servers are attacked, the biggest problem is IDS integrity, maintenance, and availability [22]. Different techniques are used to protect cloud networks from attacks, including general threat reporting, signature matching, and anomaly detection and prevention systems [23]. Cloud servers have data encryption mechanisms to protect data from unauthorized access or misuse [24]. Sensitive data encryption is a method that encrypts data and requires a decryption mechanism to access the data, after which access to the data is possible [25]. Extensive mechanisms are available to provide security to the network. These include data encryption, access control systems, data backups, authentication, and permissions.

The contribution of this paper is as follows:

Developed a tool to protect the cloud from internal and external attacks and used a Signature-Based Intrusion Detection System (SIDS) and network sensors as a gateway to protect the cloud from the external side;

Applied Signature-Based Intrusion Detection System and network sensors in parallel and monitored all malicious activity outside the network;

Applied user verification through *Access Control System* (*ACS*) if someone attacks from inside the cloud server or tries to misuse the cloud shell;

Used Cloud Shell with "*rwx-mode*" to provide internal security in which each user's access will be different from the other users;

Prevented cloud server attacks to protect the cloud servers from inside and outside attacks while comparing the existing techniques.

Problem Formulation

Various researchers have worked on different tools to protect the cloud server from attacks. Different researchers designed different algorithms and tried to protect the cloud from inside and outside attacks. Some researchers surveyed various papers, compared the techniques, datasets, and algorithms used and discussed the best techniques for detecting cloud intrusions, but no paper has experimentally proven how can the cloud be prevented from attacking inside and outside if an attacker attacks a cloud server. In this article, semi-supervised clustering will prevent internal and external attacks from the cloud server. When a user attempts to access a cloud server, the user's authenticity will be verified via network sensors and a Signature-Based Intrusion Detection System and sent to labelled or unlabeled clustering. The users who attack from outside the cloud server will be forwarded to unlabeled clustering, while the authentic users who log in with valid keys will be sent to label clustering. The reason for using the semi-supervised clustering technique is to use

different detection methods for inside and outside attacks and to develop different rules to protect the cloud server from attacks from both sides. At the end of the paper, a confusion matrix will be implemented with the different results inside and outside to evaluate the functionality of the tool, and conclusions will be drawn based on the results.

The rest of the paper is organized as follows: we discussed the related research works in Section 2. Section 3 exhibits the proposed research methodology to address the cloud security issues. However, Section 4 is devoted to the implementation of the proposal. Section 5 will compare the latest work with previous work. Section 6 concludes the paper.

2. Literature Review

Aryachandra et al. [26] proposed a network-based architecture. In this architecture, the author worked on a tool called snort. The author used two cloud servers in this network, Virtual Machine Based Rootkit-1 (VMBR1) and Virtual Machine Based Rootkit-2 (VMBR2). Virtual Machine Based Rootkit-1 and Virtual Machine Based Rootkit-2 connect the cloud server-1 with cloud server-2 using switch-2. The authors placed an IDS in three different scenarios. In the first scenario, IDS is placed outside the cloud server. In the second scenario, IDS is placed inside the cloud server. In the third scenario, the IDS is set on both sides of the cloud servers. To detect escalating attacks, eth-0 and eth-1 are used. After the placement of IDS in different scenarios, it was attacked several times. To show the performance of IDSs, they created truth tables. At the end of the paper, the authors checked the effect of the Central Processing Unit (CPU) and Random Access Memory (RAM) during the execution of snort.

Narwal et al. [27] surveyed various IoT (Internet of Things) papers and discussed how the mobile industry and the Internet have been growing too fast over the years. The set technologies have created a lot of convenience for the user, but more than that, the chances of attacks on their data are increasing. To address this issue, the system is classified into NIDS and HIDS. After that, an Architecture was developed for the set of techniques, including the stand-alone Intrusion Detection Support System, the Mutual Interference Detection Support System, and the Decentralized Intrusion Detection Support System. Discussing security of each phase is critical during the installation of the Intrusion Detection System in cloud computing. If the gateway of the Intrusion Detection System is strengthened, the number of attacks will be reduced.

Tuan et al. [28] analyzed the efficiency of various machine learning algorithms to detect inside botnet attacks. The algorithms used in this article are Support Vector Machine (SVM), Naïve Bayes, and Unsupervised Learning Algorithms. The Transmission Control Protocol (TCP) dump packet analyzer tool is used to capture the packets and extract their features. Two datasets, UNBS-NB 15 and KDD99, are used to check the efficiency of algorithms. After that, different results have been observed: Unsupervised Learning Algorithm: 94.78%, Support Vector Machine: 84.32%, and Naïve Bayes: 71.63%, and it has been concluded that Unsupervised Learning Algorithms can detect better attacks with higher accuracy.

Tadapaneni et al. [29] worked on the growing cloud security issues and how to protect the cloud from the initial level. This article explores cloud servers' security threats, vulnerabilities, and security models. The cloud can store all kinds of data and be accessed from any node. However, data security is one of the most significant growth issues in the cloud. According to the author, each technology consists of two stages. One stage leads to success, and the other stage leads to challenges. Even in the case of cloud computing, cloud end users are facing a variety of security issues. Data leaks, non-standardization, malware injections, and data breaches can lead to security issues. At the end of the paper, the significant issues of cloud computing faced by end-users and discussed some cloud threats that can damage the cloud servers.

Jyoti [30] surveyed various papers, collected and compared all the datasets and algorithms used in these papers, and discussed that an intrusion detection system is an effective tool to monitor and prevent all malicious activity on the network. The author used the Pareto principle to secure the cloud from the outside and used three effective

techniques of the Intrusion Detection System (Signature-Based Intrusion Detection System, Anomaly-Based Intrusion Detection System, Network-Based Intrusion Detection System). According to the author, attack rates will be lower if cloud servers provide external security. At the end of the paper, Signature-Based Intrusion Detection System (SIDS) results are 80.21%. In comparison, Anomaly-Based Intrusion Detection System (AIDS) results are 20.54%, while Network-Based Intrusion Detection System results are 61.23%, concluding that Signature Based Intrusion Detection Systems can provide better security than Anomaly Based and Network-Based Intrusion Detection Systems.

Wang et al. [31] used a prevention technique to secure the cloud and protect the cloud from intrusion so that the cloud could be kept as safe as possible. This article uses three algorithms to secure the Cloud: C-Kmeans, Spatial and Channel-wise Attention in Convolutional Neural Network (SCA-SNN), Principal component analysis (PCA), and lymphography and glass datasets to overcome anomaly-based detection problems. These algorithms were then applied to the datasets, and results were obtained as Kmeans: 77%, Spatial and Channel-wise Attention in Convolutional Neural Network (SCA-SNN): 88%, Principal component analysis (PCA): 67%. Finally, the Spatial and Channel-wise Attention in Convolutional Neural Network algorithm can overcome the problems of an Anomaly-Based Intrusion Detection System compared to other algorithms.

In 2021 [32], researchers developed a tool to protect cloud servers from attacks inside and outside. First, a cloud server security architecture was designed to use a separate router for each country and assign a unique IP address to each router. Second, an intrusion detection system was placed outside the cloud server, and then various attacks were carried out, such as brute force and pattern matching. Multiple techniques were discussed to prevent the cloud servers from being attacked. Third, intrusion detection systems were set up inside the cloud server, and various DDoS attacks were carried out. Different results were then applied to the confusion matrix, the External Detection Rate (EDR) was 92%, the Internal Detection Rate (IDR) was 89%, while Both side Detection Rate (BDR) was 85%. It was then concluded that, if an efficient architecture for a cloud server is developed to protect it internally and externally, the chances of an attack can be reduced. when different data points are collected into a cluster form, clustering algorithms are developed to classify these data points into different groups, and data points are divided into different categories based on these algorithms. The functionality of data points of every group is almost similar, but the functionality of each group is different from the others. Clustering techniques are unsupervised algorithm techniques. No additional data may be used to improve the outcomes of the clustering process. This study reviews articles on optimization-based semi-supervised clustering from 2013 to 2020. A four-step process is used to conduct this review in which the application domain, classification of supervised clustering, and optimization techniques are explored.

3. Proposed Algorithm

3.1. Tool Functionality

This paper will develop a tool to prevent cloud server attacks, protecting the cloud server from inside and outside attacks. Whenever an attacker tries to gain access to a cloud server, the attacker uses brute force or pattern matching techniques. This tool will protect the cloud server from external attacks like pattern matching. Whenever the user logs in to the cloud server, the user will be sent clustering for verification. Signature-Based Intrusion Detection Systems and Network Sensors will be used for verification. After verification, the user will be redirected to labelled or unlabeled clustering. If the users are valid, such users would be redirected to label clustering. Users who are invalid will be redirected to unlabeled clustering. The rules and detection mechanisms of the label and unlabeled clustering are different.

In unlabeled clustering, when the user will enter incorrect keys on the first attempt, the user will be asked to re-enter the keys. If the user still enters the wrong keys, the user's IP address will be blocked for two hours. However, still, if the attacker will attack through

the same IP address, such IP address will be permanently blocked. In Label clustering, when the user enters the cloud server, the user gets full access to the cloud server. However, in this paper, the "*rwx [r = read, w = write, x = execution]*" mode has been used to grant limited access in which each user's access will differ from the other users. Cloud Shell is designed to prevent misuse of cloud servers. By Cloud Shell, the user can access the cloud server through valid queries and use the query in "rwx-boundary". If a user enters an invalid query or tries to misuse the cloud shell query, that user will be considered an attacker and forwarded to ACS. Through ACS, the user will be verified. Suppose an invalid user enters through any key snatching method. In that case, such a user will not be able to verify the account. If an authentic user attempts to misuse the cloud server or interfere with another user's data, such a user will be alerted once, and this type of user account will be permanently blocked, and the Intrusion Detection procedure will be applied to that user. A complete methodology of proposed paper is explain in Algorithm 1.

Algorithm 1: Semisupervised Clustering

1. **Input**: *Login Keys*
2. Store keys in cluster form
3. Apply "*Network Sensor*" and "*SIDS*" mechanisms on step-2.
4. Implement "*semi-supervised clustering" on step-3*.
5. *IF* (*LOGGING_KEYS == EXISTING_KEYS*), then *GOTO* step-6.
   ELSE GOTO Step-7.
6. Use cloud shell in "*rwx-mode*".
   IF (NEW_*QUERY != EXISTING_QUERY*) then GOTO *ACS*
   IF (*ACS==SYS_EMAIL*) then *GOTO* step 6
   ELSE ((*DETECTION_MECHANISM*) && (*ACC_BLOCK*))
   ELSE GOTO step-6.
7. VERIFICATION

IF (ARRIVING_KEYS != EXISTING_KEYS), then
FUNCTION (*User_VERIFICATION_email*)
IF (*User_VERIFICATION_email != SYSTEM_EMAIL_KEY*), then GOTO "*IP_BLOCK* Function"
ELSE GOTO step-6

3.2. Network Architecture

There are two possible ways to attack a cloud server. One possibility is that the cloud server can be attacked from the outside, and another possibility is that the cloud server can be attacked from the inside. This paper will use semi-supervised clustering to distinguish valid data from invalid data, as shown in Figure 2. The user will be classified into two categories in semi-supervised clustering: labelled clustering and unlabeled clustering. Label clustering will prevent internal attacks on the cloud server, while unlabeled clustering will prevent external attacks. Whenever a user tries to login to the server, the network sensor will check the format of the keys; if the format of the keys is by the rules, then it will be sent to the Signature-Based Intrusion Detection System. The Signature-Based Intrusion Detection System will check the authenticity of the packets and send them to labelled or unlabeled clustering. In label clustering, a cloud shell will be used in which the user can access the cloud server through valid queries. The user will access the cloud server when using the correct queries. If the user uses a query, they are not allowed to use or try to use the wrong query, the user will be sent to ACS, and the user account will be verified. If the user repeatedly enters incorrect queries, the detection rules and mechanism will be implemented, and the user account will be permanently blocked.

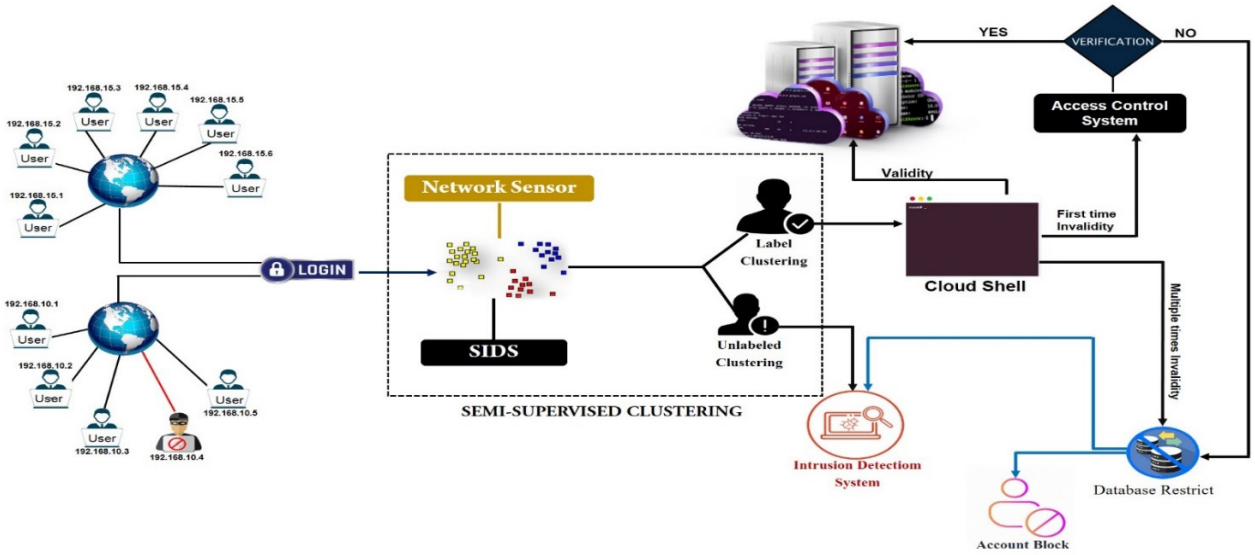

Figure 2. The architecture of Cloud Computing.

3.2.1. Semi-Supervised Clustering

Whenever valid or invalid users try to login to the cloud server or perform malicious activities, these users will be collected in a cluster form. The reason for using clustering instead of user grouping is that, when a user attempts to access cloud server data, all these users will first be collected in a cluster form so that the authenticity of the packet can be ascertained by implementing various mechanisms on this cluster data. Clustering will be used to collect and store all kinds of information, whether it is true or false, and then will classify that information based on various mechanisms.

When users try to access cloud servers from outside, security mechanisms will be used to identify the authenticity of these users. When network sensors and SIDS mechanisms are implemented on clustering data, semi-supervised clustering will be used to divide this clustering data into valid and invalid. In semi-supervised clustering, valid users will be divided into label clustering, while invalid users will be divided into unlabeled clustering. Network sensors and SIDS will be implemented on clustering to identify users' authenticity. The most significant advantage of using a semi-supervised clustering mechanism is that, whenever there is any valid or invalid activity outside of the cloud server, different security mechanisms can be used based on these activities, and these mechanisms can prevent the cloud from outside attacks.

3.2.2. Network Sensor

The function of the network sensor is to determine the format of incoming packets, meaning that the login keys entered by the user are protocols, characters, or numbers. If the user enters the protocol in the login keys, the network sensor will sense it, and the user will be prevented from going to Signature-Based and will be notified to enter the login keys. When the user enters the valid keys, the keys will be sent to the Signature-Based intrusion detection system for matching.

3.2.3. Signature-Based Intrusion Detection System (SIDS)

Whenever data are transmitted on a network, these data are transmitted in the form of patterns. When an attacker will try to inject different malicious patterns into accurate data or will perform such activities that he is not allowed to do, a Signature-Based Intrusion Detection System will be used to solve such problems. In this paper, when the network sensor will check the format of the incoming packets, the authenticity of these packets will be checked with the help of a Signature-Based Intrusion Detection System. Whenever a user logins to the cloud server or tries to access the cloud server, the incoming packet will be stored in cluster form and first the network sensor and then SIDS will be applied to that

cluster. The function of SIDS is to match the incoming packet with the existing packet and identify whether the incoming packets match the existing packets or not.

3.2.4. Label Clustering

When the user uses valid keys in the semi-supervised, it will be sent to the label clustering. Label clustering means all users can access the cloud server by entering the valid keys. Suppose an invalid user enters the correct keys by a key snatching mechanism and attacks inside the cloud server. In that case, the label clustering will respond to the user to resolve the issue. User responses will be categorized into two categories. One is the category in which the correct user misuses the data, and the second is invalid users trying to access the cloud server. These two responses will be considered negative responses. In both cases, attempts are being made to misuse the cloud server. A positive response means the user uses the cloud server correctly and does not enter the wrong queries.

3.2.5. Access Control System

Whenever an invalid user login with a snatching technique or a valid user enters the wrong query that they have no permission for, an Access Control System will be used in that case. The function of the Access Control System is to see the user's response. The Access Control System will send the user two verification steps when the user's response is invalid. The user must enter his recovery email and secret keys in two-step verification. If the two-step verification does not match the existing verification, the user will be alerted about using the cloud server. However, continuous misuse will block the user's database access, and the user account will be blocked and notify the administrator.

3.2.6. Unlabeled Clustering

When a user is invalid, it will be sent to unlabeled clustering in semi-supervised clustering. Unlabeled clustering will have all the users who are repeatedly entering invalid keys. The detection mechanism will be applied when the user's invalidity is clear. The detection method contains a set of rules which prevent the user from invalidity.

3.2.7. Detection Mechanism

When an invalid activity is performed on a cloud server, different intrusion detection mechanisms can be developed to prevent these activities, which can detect intrusion but cannot prevent intrusions that are not enough to secure the cloud entirely. In this paper, a detection mechanism will be developed in which some rules will be defined. When the user will enter the wrong keys the first time on the cloud server, he will be asked to re-enter the keys, and the verification of the keys will be done through network sensors and SIDS. The user's account will be verified when the user enters the wrong keys a second time. If the user verifies the account, he will be asked to re-enter the keys. If the user fails to verify the account, such a user will be considered an attacker, and its IP address will be blocked for 2 h, and the system administrator will be notified about the attacker's IP address, and an alert will be generated from the system. If the attacker repeatedly attacks from the same IP address, it will be blocked entirely. If the IP address is temporarily or permanently blocked on the cloud server, the attacker will never be able to attack from an address that can reduce the attack rate.

4. Experiment

4.1. Detection of Attacks outside the Cloud Server Using Semi-Supervised Clustering

Gateway security is the best way to protect cloud servers from attacks. Users must verify themselves whenever they enter a cloud server or attempt to access it. When users enter the login keys, all keys are stored in the cluster and verified according to network sensor rules. The network sensor sends the keys to the Signature-Based Intrusion Detection System for verification if the keys are in the correct format. The signature-based Intrusion Detection System matches the keys with the existing keys. If the arriving keys match

with the existing keys, then the user will be considered a valid user and sent to the label clustering, which grants access to the cloud shell. If the arriving keys do not match with the existing keys, then the user will be considered an invalid user and sent to unlabeled clustering. In Figure 3, the user accesses the cloud server via the valid keys and is sent to the label clustering, which grants access to the cloud shell.

```
[root@server]$zpx_email:m_nadeem90
[root@server]$zpx_pass:****
[root@server[PORT]]:3277
[SYS]> Please wait...
192.168.15.6 is connecting to ZPX-SERVER
$[After this operation, 425kB of additional space will be used]

connection is established successfully
[m_nadeem90]@zpx_show>
```

Figure 3. Cloud Server accessibility.

When the user entered the wrong keys on the first attempt, the server provided a second chance to re-enter the keys. If the user enters the correct keys in the second attempt, the user will have to verify the account. If the user verifies the account, the user will be sent to the label clustering, and if the user fails to verify the account, the IP address is terminated for a few hours. However, even after reopening the IP address, if the user enters the wrong keys from the same IP address, this IP address will be permanently blocked.

In Figure 4, the user used invalid keys on the first attempt. The cloud server provided a second chance to re-insert the keys. When the user entered the correct keys in the second attempt, the server verified the account and then provided the cloud shell access to the user.

```
[root@server]$zpx_email:wajia123
[root@server]$zpx_pass:****
[root@server[PORT]]:3295

find:'/etc/pks/syslog':Permission denied
find:'/etc/zrub.d':Permission denied
find:/etc/polkit-2/rules-w:Permission denied
find:/etc/polkit-2/localauthority:Permission denied
find:/etc/libvirt:Permission denied
find:/etc/SIDS:Permission denied

[root@server]$zpx_email:db_studio_pro
[root@server]$zpx_pass:****
[root@server[PORT]]:3277
[SYS]> Please wait...

[verification]#zpx-server: system_db@gmail.com
root@server[DATABASE] :Account is verified successfully.

[SYS]> Please wait...
192.168.10.3 is connecting to ZPX-SERVER
$[After this operation, 425kB of additional space will be used]

connection is established successfully
[db_studio_pro]@zpx_show>
```

Figure 4. Accessibility of cloud server in the second attempt.

When the user enters incorrect keys and cannot verify the account, the PC's IP address "*192.168.10.4*" is temporarily blocked for two hours, as shown in Figure 5.

```
[root@server]$zpx_email:wajiha_zahra786
[root@server]$zpx_pass:******
[root@server[PORT]]:3277

find:'/etc/pks/syslog':Permission denied
find:'/etc/zrub.d':Permission denied
find:/etc/polkit-2/rules-w:Permission denied
find:/etc/polkit-2/localauthority:Permission denied
find:/etc/libvirt:Permission denied
find:/etc/SIDS:Permission denied

[root@server]$zpx_email:syeda_wajiha786
[root@server]$zpx_pass:*****
[root@server[PORT]]:3277
[SYS]> Please wait...

[verification]#zpx-server: wajiha_zahra5@gmail.com

[SYS]> Please wait...
192.168.10.4 is trying to connect #ZPX-SERVER
[root@server]#System_Enable_restricted_session inet$192.168.10.4
looptxqueuelen_1000 (Local_Loopback)
[SYS]$network_status: RESTRICTED
[SYS]$DURATION: 2 Hours
```

Figure 5. Temporary IP address blocking.

When the IP address reopened two hours later, the attacker tried to enter the wrong keys. At that point, the user's IP address was permanently blocked, and a detection mechanism has been implemented, as shown in Figure 6.

```
sys>exploit[handlev]>conf_lhost 192.168.10.4
sys>exploit[handlev]>conf_lport 3277
[*]stopped reverse TCP handlev on 192.168.10.4:3277
[*]stopped the payload handler
[*]stopped stage(96251 bytes) to 15.11.6.28
syspreter> sysinfo
            Computer     : DESKTOP_31FXOFR
            OS           : Window 10(Build 10586)
            Architecture: x64
            Language     : en_US
            Domain       : WORKGROUP

[SYSTEM]~#192.168.10.4 blocked sucessfully....
```

Figure 6. Blocking of the permanent IP address.

In this paper, we try temporarily blocking the IP address to protect the cloud server from attacks because the attacker develops an attack algorithm whenever an attacker attacks the cloud server. More efficient algorithms will be needed to protect the cloud server from invading algorithms. When the attack prevention algorithm is ready, the attacker will have developed a new algorithm and attacked the cloud server. Therefore, it is better to block IP addresses temporarily and permanently. Even if the attacker applies the algorithm, the attacker's IP address will be permanently blocked before implementing this algorithm.

Prevention Techniques from External Attacks

Cloud servers can be protected from attacks in three more ways. The first way is to set the login limits on the cloud server. The second way is to encrypt the keys with hashing and salting algorithms to protect the cloud from hacking and use hashed code on the cloud server, making it difficult for the attacker to snatch the key. The third method is to use One-time password (OTP) based authentication when logging in to the cloud server, after which the user can access it.

4.2. Detection of Attacks inside the Cloud Server Using Semi-Supervised Clustering

This article focused on the command line interface rather than the Graphical User Interface (GUI) to protect the cloud server from inside attacks and provide a secure environment for data. Each user is provided limited access. Label clustering contains valid users, but thieves can come incorrectly. Many queries have been created to address this issue, and each query has been assigned a function to protect cloud data. Once a user

enters label clustering, the user can access organizations, countries, users, and files through Cloud Shell.

4.2.1. Queries for Shell

Different queries are designed for the cloud shell, as shown in Figure 7. The "*show_*org*" query will be used when the user wants to see the details of all the organizations. With the help of this query, all the organizations' details, the organizations' status, the protocols used in the organizations, and the country to which the organizations are affiliated can be seen with the help of "show_*org", as shown in Figure 8.

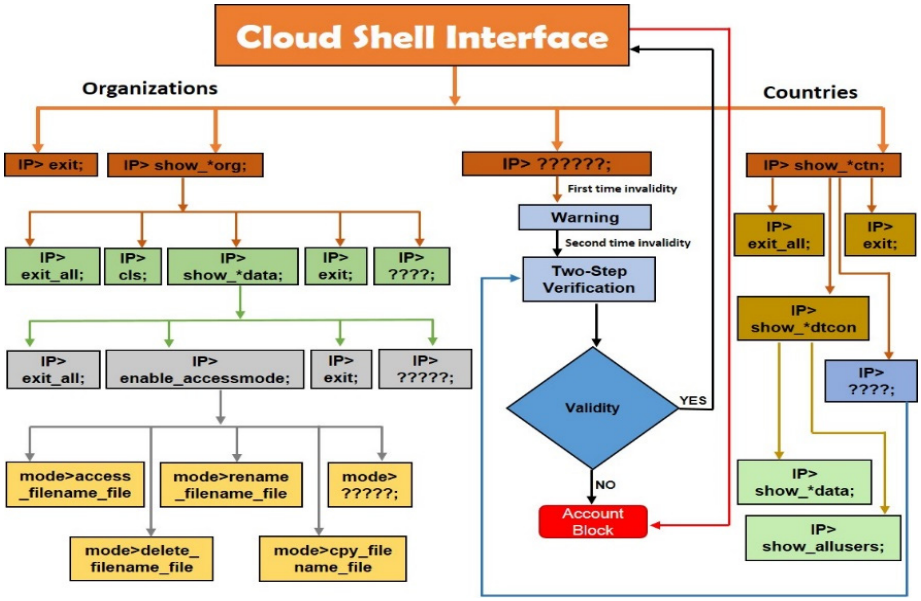

Figure 7. Cloud Shell Interface queries (* Show all organizations).

```
[sys]@zpx_show: show_*org;
 Protocol                Status              Organization              Location
-------------------------------------------------------------------------------------
 192.168.15.1            connected             Amsterdam               Netherland
 192.168.15.6            connected             Utrecht                 Netherland
 192.168.10.2            disconnected          Odesa                   Ukarine
 192.168.10.3            connected             Kherson                 Ukarine
 192.168.15.5            connected             Haarlem                 Netherland
 192.168.15.3            disconnected          Tilburg                 Netherland
 192.168.15.4            connected             Breda                   Netherland
 192.168.10.4            blocked               Poltava                 Ukarine
 192.168.10.1            connected             Rivne                   Ukarine
 192.168.15.2            connected             Enschede                Netherland
 192.168.10.5            connected             Sumy                    Ukarine
```

Figure 8. Details of all organizations.

When all the organization details are exposed to the user, the user can execute four queries on this detail. The first query is "*exit_all.*" This query will be used to exit the cloud server, as shown in Figure 9.

```
[sys]@zpx_show: show_*org;
 Protocol                Status              Organization              Location
-------------------------------------------------------------------------------------
 192.168.15.1            connected             Amsterdam               Netherland
 192.168.15.6            connected             Utrecht                 Netherland
 192.168.10.2            disconnected          Odesa                   Ukarine
 192.168.10.3            connected             Kherson                 Ukarine
 192.168.15.5            connected             Haarlem                 Netherland
 192.168.15.3            disconnected          Tilburg                 Netherland
 192.168.15.4            connected             Breda                   Netherland
 192.168.10.4            blocked               Poltava                 Ukarine
 192.168.10.1            connected             Rivne                   Ukarine
 192.168.15.2            connected             Enschede                Netherland
 192.168.10.5            connected             Sumy                    Ukarine

[sys]@zpx-show:exit_all;
Please wait....
SYSTEM is disconnected.
```

Figure 9. Exit function.

The second query is "*cls*", whose job is to clear the screen. With this query's help, all the organizations' details will disappear from the screen. The third query is "*show_*data,*" which will show the data of all organizations, as shown in Figure 10.

```
[sys]@zpx-show:show_*data;
total 162

1          192.168.15.1          Aug          7          08:41          Win10.GHO
2          192.168.15.3          Oct          24         09:50          DPS.exe
3          192.168.10.6          Oct          21         04:22          PL/SQL.pdf
4          192.168.10.2          Sep          15         19:45          DLCD.exe
5          192.168.10.5          Aug          09         20:41          python3.9.0.exe
6          192.168.15.1          Aug          24         15:59          Win10_AIO_ENU_2019.ISO
7          192.168.15.1          Sep          22         19:32          VS-x64-1.52.exe
```

Figure 10. Files of all organizations.

If the user wants to access a file, the user must first enable the access mode for which the "*enable_access mode*" query will be used; then, the files may be accessible, as shown in Figure 11.

```
161          192.168.10.3          oct          14          18:24          wps_office.exe
162          192.168.15.6          aug          07          21:07          refus_3.7p.exe
[sys]@zpx-show:enable_accessmode;
mode:changing permission to -rx mode
mode:permission changed successfully
```

Figure 11. Change the mode of files.

Some queries are allowed to users in the cloud server, and some are denied to users so that users can only access data and not make changes to other users' files, as shown in Figure 12.

```
161          192.168.10.3          oct          14          18:24          wps_office.exe
162          192.168.15.6          aug          07          21:07          refus_3.7p.exe
[sys]@zpx-show:delete-vs-x64-1.52.exe;
InvalidRequest:[permission denied]
[sys]@zpx-show:
```

Figure 12. Wrong query.

The query "*show_*ctn*" will be used when a user wants to view all the countries connected to the cloud server; the query "*show_*ctn*" will be used, as shown in Figure 13.

```
[sys]@zpx-show:show_*ctn;
No          Countries          Port          Code          Users          Status
1           Natherland         3277          +31             6           connected
2           Ukarine            3295          +380            6           connected
[sys]@zpx-show:
```

Figure 13. Countries connected to cloud servers.

When a user tries to use the wrong queries on a cloud server, this response will be considered a negative response. This response can be from the correct user side or the

invalid user side when the valid user tries to misuse the queries or use such queries that are not allowed. In this case, the user will be alerted, and the user will be blocked due to repeated use of incorrect queries, as shown in Figure 14.

```
[sys]@zpx-shell:show_organization;
InvalidRequest:[permission denied]
[sys]@zpx-show:show_*organization
InvalidRequest:[permission denied]
zpx-00240:unknown command:/etc/home/emoh$/uinstitucion/cms.dbf
zpx-04206:unknown command:exploit
Try 'root --help' for more informations,message,=[verification required]
[verification]-zpx-account:syeda.wajia786@gmail.com
[verification]-zpx-pass:*****
[root@server]$zpx_DATABASE:Account verification completed successfully
[sys]@zpx-show:show*_org;
InvalidRequest:[permission denied]:RESTRICTED_SESSION_enable
restrict:192.168.10.3 mask 255.255.255.0 nomodifynotrap
restrict:database_SERVER nomodify nopeer
restict:127.0.0.0
restrict::1
restrict:/etc/pks/syslog:permission denied
restrict:/etc/zpx-smtp:permission denied
restrict:/etc/zpx-imap:permission denied
restrict:/etc/zpx-ssh:permission denied
Account Blocked:YES
IPV4PROT:RESTRICTED
[SYSTEM]~#192.168.10.3 locked permanently
```

Figure 14. Account Block in case of invalid queries.

This article uses Cloud Shell to protect the cloud server from internal attacks. If the attacker gains access to the cloud server but does not know the exact query, the attacker can be easily identified. If a valid user tries to tamper with other users' data, that user's account is blocked. If mechanisms were created to secure the cloud server, the attacker devised more attacks than security mechanisms. Cloud Shell is an efficient technique in which every user can be given limited access, and each user will be able to stay within their limits. It will not know other users' queries, nor will it be able to destroy anyone else's data.

4.2.2. Prevention Techniques from Internal Attacks

There are three ways to protect the cloud server from internal attacks. The first way is to use the cloud shell on the server using the "rwx" mode as used in this paper. The second way is to store the data in an encrypted form. If a user wants to access data, the user can only do so with the decryption key of their data. The advantage is that no user will access another user's data. The third way is that, if an attacker tries to gain access to the cloud through malicious activity, these activities will be blocked through Cloudflare.

4.3. Implementation of Semi-Supervised Clustering Results in the Confusion Matrix

Check the demonstration performance of the proposed semi-supervised clustering technique on the dataset shown in Table 2 using 5-fold cross-validation. Some of the parameters used for testing the confusion matrix are as follows:

Table 2. Results of Label and Unlabeled Semi-Supervised Clustering.

Testing = 100		**ACTUAL**	
		Intrusive (+ve)	Not Intrusive (+ve)
TOOL	Intrusive (+ve)	TP = 62	FP = 2
PREDICTION	Not Intrusive (+ve)	FN = 3	TN = 33

TP (True Positive): True Positive means arriving packets are intrusive, and the tool predicts it correctly;

FN (False Negative): The arriving packets were intrusive, and the tool did not predict them correctly;

TN (True Negative): True Negative means that arrival packets were not intrusive, and the tool declared that arriving packets are not intrusive;

FP (False Positive): Packets that were not intrusive, but the tool found them to be intrusive.

4.3.1. Evaluation

After obtaining results, these results have been applied to the confusion matrix to obtain the instrument's performance in which the accuracy has been evaluated.

Positive Prediction

The Positive Prediction (*PP*) indicates a positive probability of an outcome. This means how likely it is to detect *intrusion* from *intrusive packets*:

$$PP = \frac{TP}{TP + FP} PP = \frac{62}{62 + 2} = 96.87\%$$

Negative Prediction

The Negative Prediction (*NP*) indicates a negative probability of an outcome. This means the probability that incoming packets are *authentic* and have *no intrusion*.

$$NP = \frac{TN}{FN + TN} NP = \frac{33}{3 + 33} NP = 91.67\%$$

After finding the positive and negative predictors, it has been discussed that, when intrusive activities have been performed on a cloud server, the intrusion detection rate of the tool has been 96.87%, while when authentic packets are transmitted on a cloud server, the tool's authenticity rate has been 91.67%.

Tool Accuracy

The proportion of correctly predicted data points out of all data points is known as accuracy. Accuracy indicates how often the model was correct or how well it worked:

$$TA = \frac{TP + TN}{TP + TN + FP + FN}$$

$$TA = \frac{62 + 33}{62 + 33 + 2 + 3}$$

$$TA = \frac{95}{100}$$

$$TA = 95\%$$

The datasets have been implemented on the confusion matrix to check the tool's efficiency, and then different results have been obtained in which the tool accuracy was 95%. If different mechanisms for label clustering and unlabeled clustering are used in this tool, the attack rate in the cloud server can be further reduced.

K-Fold Cross Validation

In this article, 100 different samples of datasets have been taken, and these datasets have been applied to K-fold cross-validation in which the value of K is taken as 5, and then five times iterations have been done. After that, different results have been obtained by applying different formulas, and the performance of the tool has been identified, as shown in Table 3: Sensitivity (Se), Precision (Pr), Accuracy (Acc), Specificity (Sp), and Error Rate (ER).

Table 3. Comparative analysis of accuracy.

Fold Iterate	TP	FP	TN	FN	Se	Pr	Acc	Sp	E.R	F1
1	70	3	25	2	97	95	95	89	5	95
2	65	1	31	3	97	98	96	96	4	97
3	61	7	27	5	92	89	88	79	12	90
4	63	8	23	6	91	88	86	74	14	89
5	55	5	32	8	87	91	87	86	13	88
Mean	62.8	4.8	27.6	4.8	92.8	92.2	90.4	84.8	9.6	91.8
SD	5.4	2.8	3.8	2.3	4.2	4.2	4.7	8.5	4.7	3.9

After obtaining the different results, it is discussed that data can be stored in a clustered form with the help of semi-supervised clustering. These clustered data can be divided into different categories by implementing some semi-supervised mechanisms. This paper uses semi-supervised clustering to protect data from internal and external side attacks. Different mechanisms can be implemented when someone tries to access a cloud server based on the user's behaviour. The attack rate can be completely determined if more algorithms are used. The most significant advantage of semi-supervised clustering is that each clustered value can be stored. Clustered means storing all user's records, whether valid or invalid and dividing them into different categories based on these records. A cloud server can be secured internally and externally if semi-supervised clustering is used efficiently, and different mechanisms can be applied to each user behaviour.

5. Comparative Analysis

Many researchers have designed different algorithms to secure the cloud servers and have developed many tools to reduce the attacking ratio from the cloud servers. Some researchers have surveyed most of the papers and tried to implement the best techniques to secure the cloud servers, but as the number of users in the cloud has increased, the attack ratio has also increased. If the cloud administrator has designed an encryption algorithm to secure the cloud data, the attackers have created a more efficient decryption algorithm to decrypt that data. Based on these, the attack ratio increased rather than decreased. A comparative analysis of the latest is shown in Table 4.

Table 4. Comparative analysis of techniques.

Sr#	1	2	3	4	5	Proposed Work
Reference No.	[26]	[28]	[30]	[31]	[32]	
Year	2016	2020	2020	2021	2021	
Outside Security Techniques	IDS Server, vmbr1, vmbr2	✗	SIDS, AIDS	✗	HIDS, NIDS	SIDS, Network Sensor
Inside Security Techniques	IDS Server, vmbr1, vmbr2	Used *TCP dump* packet analyzer tool to extract features from packets	✗	Anomaly Based IDS	Cloudflare, Cloud Shell	Access Control System, Cloud Shell
Algorithm	Worked on a tool named Snort	Support Vector Machine, Naïve Bayes, Unsupervised Learning	Pareto principle	C-K means SCA-SNN, PCA, HC (Datasets: Lymphography, Glass)	Implemented Cloud Shell and Cloudflare to protect from attacks	Semi-supervised Clustering
Novelty	IDS can detect attacks from both sides at a time	Unsupervised Leaning can detect better attacks as compared to other algorithms	Signature-Based IDS is better than Anomaly Based IDS	Overcome the Anomaly Based Detection problem	Authentic users can access data through authoritative queries, while Cloudflare can reduce DDoS attacks.	User validation, User-Limitation, Queries-based interface

In 2016 [26], researchers placed the Intrusion Detection System inside and outside the cloud server to protect the cloud server from attacks from both sides. They used Virtual Machine Based Rootkit-1 and Virtual Machine Based Rootkit-2 to connect the cloud server to different devices and worked on a tool to implement an Intrusion Detection System. They confirmed that IDS could be used to prevent cloud server attacks and concluded that, when an Intrusion Detection System is activated on the server, it will be only 2.5%. In 2019 [27], researchers worked on three algorithms to protect the cloud server from botnet attacks, used the TCP dump packet analyzer to extract features from botnet packets, and obtained different results in unsupervised learning 94.78%, support vector 84.32%, while Naive Bayes is 71.63%. A comparative analysis between previous work results with the latest work results is shown in Table 5.

Table 5. Comparative analysis of the accuracy of algorithm results.

		[28]			[30]			[31]			[32]		Proposed Work		
Algorithm	**UL**	**SVM**	**NB**	**SIDS**	**AIDS**	**NIDS**	**SCA**	**CK**	**PCA**	**EDR**	**IDR**	**BDR**	**PP**	**NP**	**TA**
Results	94.78	84.32	71.63	80.21	20.54	61.23	88	77	67	92	89	85	96.87	90.62	94.79
Mean		83.57			53.99			77.33			88.66			94.09	
SD		11.59			30.48			10.50			3.51			3.18	

In 2020 [28], authors surveyed various papers, collected all the data sets used in these papers, and discussed whether, if all these techniques are implemented in the intrusion detection system, the cloud server can be prevented from attacks. In 2021 [29], the authors used outlier detection and semi-supervised clustering algorithms to secure cloud servers and used some real data sets on these algorithms. After that, lymphography and glass were used to perform simulations, and the algorithms' novelty was observed. However, no paper has experimentally proven how a cloud server can be protected from an attack if a cloud server is attacked, nor has any paper proved how this mechanism be avoided if an attacker on a cloud server uses a mechanism,.

5.1. Statistical Analysis

We carried out a one-way ANOVA test shown in Table 6, to determine the statistical significance for observed performance results. The test was applied at $\alpha = 0.05$ significance level. The testing hypotheses are

Table 6. ANOVA test.

	df	**Sum of Sq**	**Mean Sq**	**F-Value**	***p*-Value**
Algorithm	4	47.280	11.82	15.196234	7.16×10^{-5}
Residual	63	49.003	0.778		

The *p*-value is a probability of observing a test statistic as extreme as the one authentically observed. The more minute the *p*-value, the more vigorously the tests reject the null hypothesis. In our example, the *p*-value 7.16×10^{-5} is much smaller than α, and the result is null hypothesis Ho is rejected. We can conclude that there is at least one approach amongst six approaches that significantly outperforms the others.

Ho: The performance is the same among the five algorithms across the datasets;

Ha: At least one of the performances of the algorithm is significantly better than the other algorithms.

5.2. Validation Test

This article discusses various techniques used to protect cloud servers from attacks and implement these techniques' functionality on the tool.

The user should be thoroughly checked before granting access to the cloud server for the Signature-Based Intrusion Detection System and network sensors.

When an invalid user accesses the cloud server, Cloud Shell should be used to prevent that user from accessing the cloud server.

Attacks can be minimized by using Cloud Shell because only the correct query on Cloud Shell can give the user access, and the boundaries of each query should be defined. When a user uses an incorrect query or crosses boundaries, the user can be checked via ACS.

If each mechanism is implemented inside and outside the cloud server, as discussed in this article, the chances of attacking the cloud server may be reduced.

5.3. Novelty of Proposed Work

This paper protected the cloud server internally and externally through efficient clustering techniques and prevented attacks from both sides. If an attacker gains access to a cloud server through an algorithm or a key snatching method, then the biggest problem for the attacker is that it needs to know the exact queries. When the wrong person enters the invalid keys, it is verified whether the person who has access to the cloud is right or wrong. If the correct user uses queries that the database administrator has denied or attempted to modify, such users are also blocked from cloud servers. If an attacker attacks the cloud server from outside, the IP address of that user will be blocked based on different rules. The most significant advantage is that, as long as the attacker misuses the cloud server, the attacker's IP address will be blocked. After that, the confusion matrix was used to better evaluate the instrument's performance, with a positive prediction result of 96.87%, a negative prediction result of 90.62%, and a tool accuracy result of 94.79%. This means that the tool's ability to check unauthorized incoming packets and their intrusion is 96.87%, the tool's ability to check authentic packets is 90.02%, and the tool's performance is 94.79%. Based on the confusion matrix, it has been decided to protect the cloud server from internal and external attacks and to protect the cloud by replacing the graphical user interface with a command-line interface, and as soon as an attack occurs, detect it and be saved from the attack immediately.

6. Conclusions

The development and testing of the tool have shown that the intrusion detection system is a technique that monitors all malicious activities in the cloud and prevents all attacks in the cloud. The cloud server can only be secured when given an initial level of security, every phase of the cloud server is secured, and all devices connected to the cloud server are secured. When an attacker tries to attack a cloud server, the first step is to attack the gateway. If an attacker gains access to the cloud server, it is also essential to protect it internally. The best way is CLI (Command Line Interface). This is because, if the wrong person uses the invalid queries, such people will automatically get stuck, and the performance of cloud computing will not be affected.

In this paper, we designed a security architecture and developed a tool to implement it, which provides security to the internal and external sides of the cloud. We observed the tool's performance based on Confusion Matrix and concluded that internal attacks could be reduced if the cloud algorithm is externally secured. This is because external attacks are always attempted by an unauthorized person who uses attacking techniques and tries to reach the cloud.

In the future, we will modify the semi-supervised algorithm and will develop a more secure and efficient semi-supervised clustering algorithm that will completely prevent the cloud servers from both sides attacks. This paper proposed an algorithm that protects the cloud server from outside through a detection mechanism and IP blockage mechanism, and protects the cloud server from inside attacks through cloud shell, ACS mechanism, and detection mechanism. The proposed algorithm cannot protect the cloud server from various attacks such as Brute force, DDoS, and Replay attacks, which is the limitation of this paper's proposed method. In future work, the latest algorithm will detect and prevent all possible attacks inside and outside. After that, we will compare this algorithm with different algorithms and work out the best algorithm among them. Furthermore, we

will check the effect of the Random Access Memory and Central Processing Unit while implementing the semi-supervised clustering algorithm.

Author Contributions: M.N. Conceptualization; A.A. Software, Writing—review and editing; S.W.Z. Methodology; S.R. Writing—review and editing; A.K.D. Editing; S.A. funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Researchers Supporting Program (TUMA-Project-2021-27) Almaarefa University, Riyadh, Saudi Arabia.

Acknowledgments: The authors deeply acknowledge the Researchers supporting program (TUMA-Project-2021-27) Almaarefa University, Riyadh, Saudi Arabia for supporting steps of this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ustebay, S.; Turgut, Z.; Aydin, M.A. Intrusion detection system with recursive feature elimination by using random Forest and deep learning classifier. In Proceedings of the 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 3–4 December 2018; pp. 71–76.
2. Vishal, V.; Vasudha, K. DOS/DDOS Attack Detection using Machine Learning: A Review. In Proceedings of the International Conference on Innovative Computing & Communication (ICICC), Delhi, India, 20–21 February 2021.
3. Jyoti, N.; Behal, S. A Meta-evaluation of Machine Learning Techniques for Detection of DDoS Attacks. In Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 17–19 March 2021.
4. Qin, Z.; Liu, D.; Hua, H.; Cao, J. Privacy Preserving Load Control of Residential Microgrid via Deep Reinforcement Learning. IEEE Transactions on Smart Grid. *IEEE Trans. Smart Grid* **2021**, *12*, 4079–4089. [CrossRef]
5. Ganti, V.; Yoachimik, O. DDoS Attack Trends for 2021 Q2, The Cloudflare Blog, July 2021. Available online: https://blog.cloudflare.com/ddos-attack-trends-for-2021-q2/ (accessed on 15 May 2022).
6. Li, X.; Chen, W.; Zhang, Q.; Wu, L. Building auto-encoder intrusion detection system based on random forest feature selection. *Comput. Secur.* **2020**, *95*, 101851. [CrossRef]
7. Kasongo, S.M.; Sun, Y. A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Comput. Secur.* **2020**, *92*, 101752. [CrossRef]
8. Dong, S.; Xia, Y.; Peng, T. Network Abnormal Traffic Detection Model Based on Semi-Supervised Deep Reinforcement Learning. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 4197–4212. [CrossRef]
9. Dargan, S.; Kumar, M.; Ayyagari, M.R.; Kumar, G. A Survey of Deep Learning and Its Applications: A New Paradigm to Machine Learning. *Arch. Comput. Methods Eng.* **2020**, *27*, 1071–1092. [CrossRef]
10. Seals, T. The Second Quarter of the Year Saw the Highest Volumes of Ransomware Attacks ever, with Ryuk Leading the Way, August 2021. Available online: https://threatpost.com/ransomware-volumes-record-highs-2021/168327/ (accessed on 15 June 2022).
11. Toh, A. Azure DDoS Protection—2021 Q1 and Q2 DDoS Attack Trends, August 2021. Available online: https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q1-and-q2-ddos-attack-trends/ (accessed on 12 July 2022).
12. Ji, H.; Wang, Y.; Qin, H.; Wang, Y.; Li, H. Comparative Performance Evaluation of Intrusion Detection Methods for In-Vehicle Networks. *IEEE Access* **2018**, *6*, 37523–37532. [CrossRef]
13. Ates, C.; Ozdel, S.; Anarim, E. Clustering Based DDoS Attack Detection Using the Relationship between Packet Headers. In Proceedings of the 2019 Innovations in Intelligent Systems and Applications Conference, ASYU, Bornova, Turkey, 31 October–2 November 2019; pp. 1–6.
14. Kaur, G.; Gupta, P. Hybrid Approach for detecting DDOS Attacks in Software Defined Networks. In Proceedings of the 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 8–10 August 2019; pp. 1–6.
15. Zhang, J. Detection of network protection security vulnerability intrusion based on data mining. *Int. J. Network Secur.* **2019**, *21*, 979–984.
16. Tama, B.A.; Comuzzi, M.; Rhee, K. TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System. *IEEE Access* **2019**, *7*, 94497–94507. [CrossRef]
17. Firch, J.; Kimmel, S.; Selvidge, R.; Allen, J. Cyber Security Statistics The Ultimate List of Stats Data, & Trends For 2022. Available online: https://purplesec.us/resources/cyber-security-statistics/ (accessed on 12 July 2022).
18. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 20. [CrossRef]
19. Khraisat, A.; Gondal, I.; Vamplew, P. An anomaly intrusion detection system using C5 decision tree classifier. In *Trends and Applications in Knowledge Discovery and Data Mining*; Springer International Publishing: Cham, Switzerland, 2018; pp. 149–155.
20. Lyngdoh, J.; Hussain, M.I.; Majaw, S.; Kalita, H.K. An intrusion detection method using artificial immune system approach. In Proceedings of the International Conference on Advanced Informatics for Computing Research, Shimla, India, 14–15 July 2018; pp. 379–387.

21. Ghasempour, A. Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. *Inventions* **2019**, *4*, 22. [CrossRef]
22. Haghighat, A.T.; Shajari, M. Service integrity assurance for distributed computation outsourcing. *IEEE Trans. Serv. Comput.* **2020**, *13*, 1166–1179.
23. Tan, L.; Pan, Y.; Wu, J.; Zhou, J.; Jiang, H.; Deng, Y. A new framework for ddos attack detection and defense in sdn environment. *IEEE Access* **2020**, *8*, 161908–161919. [CrossRef]
24. Karaçay, L.; Savaş, E.; Alptekin, H. Intrusion detection over encrypted network data. *Comput. J.* **2020**, *63*, 604–619. [CrossRef]
25. Aryachandra, A.A.; Arif, Y.F.; Anggis, S.N. Intrusion Detection System (IDS) server placement analysis in cloud computing. In Proceedings of the 2016 4th International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, 25–27 May 2016.
26. Narwal, P.; Kumar, D.; Singh, S.N. A hidden markov model combined with markov games for intrusion detection in cloud. *J. Cases Inf. Technol.* **2019**, *21*, 14–26. [CrossRef]
27. Tuan, T.A.; Long, H.V.; Son, L.H.; Kumar, R.; Priyadarshini, I.; Son, N.T.K. Performance evaluation of Botnet DDoS attack detection using machine learning. *Evolut. Intell.* **2020**, *13*, 283–294. [CrossRef]
28. Tadapaneni, N.R. Cloud computing security challenges. *Int. J. Innov. Eng. Res. Technol.* **2020**, *7*, 1–6.
29. Snehi, J. Diverse methods for signature based intrusion detection schemes adopted. *Int. J. Recent Technol. Eng.* **2020**, *9*, 44–49. [CrossRef]
30. Wang, Y.; Ma, J.; Sharma, A.; Singh, P.K.; Gaba, G.S.; Masud, M.; Baz, M. An Exhaustive Research on the Application of Intrusion Detection Technology in Computer Network Security in Sensor Networks. *J. Sens.* **2021**, *2021*, 5558860. [CrossRef]
31. Nadeem, M.; Arshad, A.; Riaz, S.; Band, S.S.; Mosavi, A. Intercept the Cloud Network From Brute Force and DDoS Attacks via Intrusion Detection and Prevention System. *IEEE Access* **2021**, *9*, 152300–152309. [CrossRef]
32. Ghasemi, Z.; Khorshidi, H.A.; Aickelin, U. A survey on Optimization-based Semi-supervised Clustering Methods. In Proceedings of the 2021 IEEE International Conference on Big Knowledge (ICBK), Auckland, New Zealand, 7–8 December 2021.