Computers, Materials & Continua
DOI: 10.32604/cmc.2023.028796
Article

Preventing Cloud Network from Spamming Attacks Using Cloudflare and KNN

Muhammad Nadeem[1], Ali Arshad[2], Saman Riaz[2], SyedaWajiha Zahra[1], Muhammad Rashid[2], Shahab S. Band[3,*] and Amir Mosavi[4,5,6]

[1]Department of Computer Science, Abasyn University, Islamabad, 44000, Pakistan
[2]Department of Computer Science, National University of Technology, Islamabad, 44000, Pakistan
[3]Future Technology Research Center, National Yunlin University of Science and Technology, Douliu, Yunlin, 64002, Taiwan
[4]Institute of Information Society, University of Public Service, Budapest, 1083, Hungary
[5]John von Neumann Faculty of Informatics, Obuda University, Budapest, Hungary
[6]Institute of Information Engineering, Automation and Mathematics, Slovak University of Technology in Bratislava, Slovakia
*Corresponding Author: Shahab S. Band. Email: shamshirbands@yuntech.edu.tw
Received: 18 February 2022; Accepted: 25 May 2022

Abstract: Cloud computing is one of the most attractive and cost-saving models, which provides online services to end-users. Cloud computing allows the user to access data directly from any node. But nowadays, cloud security is one of the biggest issues that arise. Different types of malware are wreaking havoc on the clouds. Attacks on the cloud server are happening from both internal and external sides. This paper has developed a tool to prevent the cloud server from spamming attacks. When an attacker attempts to use different spamming techniques on a cloud server, the attacker will be intercepted through two effective techniques: Cloudflare and K-nearest neighbors (KNN) classification. Cloudflare will block those IP addresses that the attacker will use and prevent spamming attacks. However, the KNN classifiers will determine which area the spammer belongs to. At the end of the article, various prevention techniques for securing cloud servers will be discussed, a comparison will be made with different papers, a conclusion will be drawn based on different results.

Keywords: Intrusion prevention system; spamming; KNN classification; spam; cyber security; botnet

1 Introduction

Cloud computing is a centralized data storage system where the user stores all types of data [1], and this data can be accessed from any part of the world. Cloud computing consists of three basic layers [2]. The first layer is the system layer in which all types of servers and their connections are established and maintained. The second layer is the platform layer in which all kinds of operating

systems run. The third layer of cloud computing is the application layer. All cloud applications run in this layer. Software layersare always offered to end-users [3]. The hardware layer does not include and is not offered to end-users.

Cloud computing and artificial intelligence are two emerging technologies [4]. Nowadays, a large amount of data is generated, and it is better to access the data from different technical devices like Hard Disk, CDs, DVDs rather than cloud servers [5]. Various organizations use the cloud for other purposes and store data [6]. With the development of technology, the usage of cloud computing is increasing [7]. Cloud computing offers three kinds of models [8] which satisfy the business requirements, these are known as:

- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)

Approximately 81% of companies worldwide depend on the cloud [9]. Different service providers implement other security mechanisms in the cloud, but the attackers still attack the cloud [10]. Many organizations have focused on securing the cloud server from the external side and discussed many mechanisms. However, most of the attacks on the cloud server are from inside [11]. The Intrusion Detection System is considered a better technique for securing the cloud server from outside. This technique has attracted a lot of researchers [12]. An intrusion Detection System is a techniqueused to detect the intruder's attacks and see where the attack arises from. An intrusion detection system can monitor malicious activities inside and outside the cloud network [13]. There is a wide variety of intrusion detection tools available in antivirus that can detect and monitor the traffic or malware and prevent data from being attacked [14]. The attacker always targets different devices and tries to access various devices to misuse them, as shown in Fig. 1.

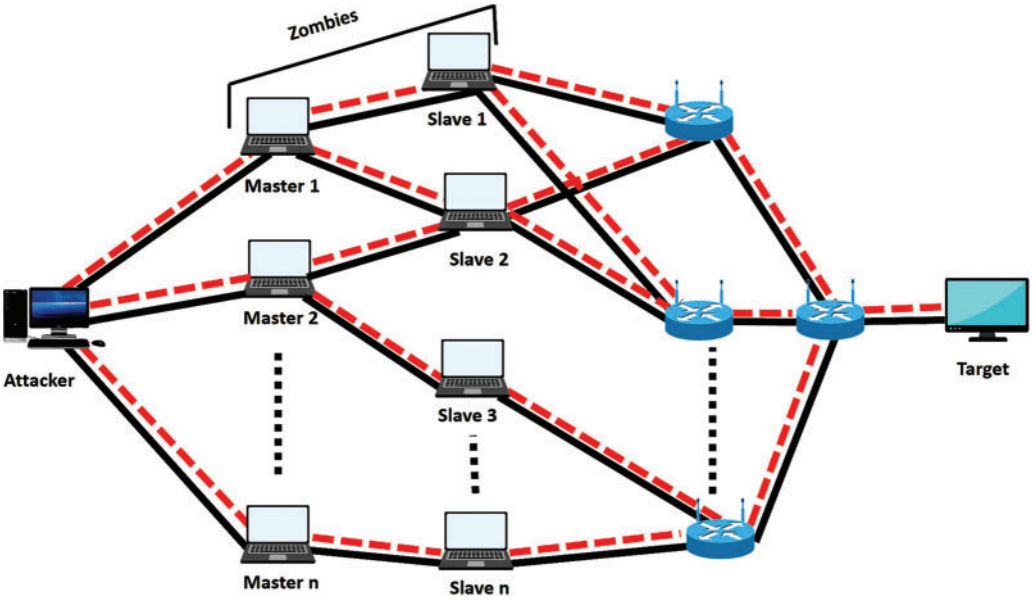

Figure 1: Spamming attack

End users store all kinds of data in the cloud. As well as, cloud security is also important for the cloud [15]. Different types of algorithms, tools, and techniques have been developed for protecting

the cloud. An intruder host tries to attack the cloud and uses various techniques, tools to snatch the data. Various types of tools are developed for detecting intrusions [16]. Some are snort, Suricata, Open Source HIDS Security (OSSEC), and Zeek.

Many organizations secure cloud servers from the outside however most attacks on the cloud server are from inside [17]. The cloud server can be protected from outside attacks but it is very difficult to detect inside attacks and protect the cloud from them. Many algorithms are available to protect the cloud from attacks, but very few solutions have managed to protect the cloud server from attacks.Internal and external security is essential for saving data on cloud servers [18]. Whenever an attacker attacks a cloud server from the outside, it can be stopped, but when an attack occurs inside a cloud server, it is difficult to stop the attack [19]. Authentic users carry out an internal attack on the cloud server. Whenever a user has accessed the cloud server, whether the user is authentic or unauthentic, it has accessed the entire cloud server, and he can attack any cloud server node. The most common attacks within cloud servers are spamming, Distributed Denial-of-Service (DDoS), and phishing [20].

As the number of users on the cloud network increases and organizations move their business to the cloud, security for cloud networks is also becoming more important [21]. Various mechanisms are developed to secure the network, including authentication, authorization, data encryption, access control system, data backup [22]. But with the help of these mechanisms, the cloud network cannot be completely secured.

The intrusion of an attacker on a network is not uncommon; each intrusion has some mechanism that can cause an attack. Cloud servers are always attacked internally by spamming [23]. Spamming is a technique that lures end-users and offers different offers depending on the user's requirement. These offers include techniques or algorithms that attack end-users when they accept offers and destroy user data. There are fewer solutions that have been properly implemented to prevent spamming and there are other algorithms that, if implemented, can prevent spamming as used in this paper.

Cloud server attacks are carried out through various spamming categories, including common vishing, baiting, bots, and DDoS [24]. Whenever, there is an internal attack on the cloud server that is in two scenarios. One scenario is that a person gains unauthorized access to the cloud and does different types of spamming to misuse cloud data. The second scenario is that an authorized person attacks inside the cloud server. Both scenarios are aimed at manipulating or misusing cloud server data. Attacks outside the cloud server can be prevented but it is very difficult to prevent internal attacks and secure the cloud server from such attacks.

In this paper, the existing tool [25] has been updated to prevent the cloud server from internal spamming attacks. The attacker's PC's static and dynamic IP address will be blocked due to spamming using Cloudflare, and the authentic user will have access to the cloud server. After that, the KNN classification will be used to locate the attacker, which can identify the attacker's location. Some other blocking techniques will be discussed which can block the cloud server from inside.

The rest of the paper is arranged as follows. Section 2 will briefly review recent developments, Section 3 will introduce the new proposed methodology, Section 4 will describe the experimental results and analysis, and Section 5 will conclude the paper.

2 Literature Review

According to the researcher [24], the main reason for various attacks on cloud servers is the lack of initial security. To address these issues, the attackers worked on various security challenges. They

discussed various tactics to secure the cloud infrastructure, including some security models, risks, and threats associated with cloud servers. According to the author, every technology has two stages. One stage leads to challenges, while the other stage leads to prosperity. Along with cloud computing, cloud users face various security challenges. Security issues can arise for several reasons, such as insider attacks, lack of support, and standardization. Afterward, researchers discussed some security issues and privacy leakage that cloud users face and some threats and risks associated with data stored on the cloud.

As the ratio of botnet attacks increases on Internet of Things (IoT), the botnet prevention capability of the Intrusion Detection Sysytem (IDS) reduces [25]. By taking advantage of these botnets, the attacker slows down the network's performance and even turns every device into a zombie. This article used the "Baptized BotIDS" technique based on the Deep Learning Convolutional neural network to solve this problem. First, some Bot-IoT datasets have been taken, and these datasets have been tested on some bots. After that, the correct BotIDS results were 99.94%, with a confirmation loss of 0.58% and an implementation time of less than 0.34 ms.

According to researchers [26], spam messages are junk messages sent to a node in large quantities via electronic medium. Most spam messages are annoying and have viruses attached to them, which can be harmful to the cloud server. To solve this problem, researchers wanted to identify and separate junk messages from regular messages, so they took four different datasets and implemented these datasets with two deep learning algorithms. Attempts were then made to find some words that were repeatedly used in spam messages, and it was discussed that if the keywords of spam messages are searched, then personal information can be saved from spam.

In paper [27], A tool was developed to protect the cloud server from internal and external attacks. Various techniques have been implemented to protect the cloud server from brute force and pattern matching attacks, and various techniques have been discussed to protect the cloud server from internal attacks like DDoS. After obtaining different external attack results, these results were implemented on commutative law and identity property. Moreover, it has been argued that if the cloud server is to be protected from internal and external attacks, then all efficient algorithms are to be practically applied to the cloud server, which will significantly reduce the chances of an attack.

As users store large amounts of data on cloud servers [28], cloud threats are complex for current systems to understand. Different techniques were compared to solve this problem, and an efficient Network-based Intrusion Detection System was developed. Subsequently, various UNSW-NB datasets were taken, and the feature was selected based on these datasets. An AdaBoost-based approach was proposed to detect network interference based on these features. UNSW-NB datasets include nine types of attacks: DoS, Fizzers, Exploit, Worm, shellcode, reconnaissance, generic, and analysis Backdoor. After that, comparisons were made using Support Vector Machine (SVM) and Multilayer Perception (MLP), and discussion was held that the proposed method detected network intrusions and attained an accuracy of 99.3% using the UNSW-NB15 dataset.

In this paper [29], a 3D watermarking algorithm based on wavelet is proposed to establish safe transmission and storage of medical data. This algorithm minimizes data dimension by using the principal component analysis (PCA) transform, which can minimize the error between original data and extracted components. After that, some experiments were done using MATLAB software based on standard MRI brain volume datasets and discussed that the proposed algorithm has efficient robustness and slightly distorts the 3D model after embedding the watermark. The simulation results show that the proposed method has strong robustness and can withstand geometric attacks.

In this paper [30], a two-stage reversible robust audio watermarking algorithm has been proposed to avoid leakage of patient information in telemedicine. The scheme divides medical audio into two independent domains and embeds robust watermark and reversible watermark in two domains, respectively. Hurst exponent has been used for audio quality. After that, some simulations have been done and discussed that this scheme has efficient imperceptibility and robustness to MP3 compression, AWGN, low pass filtering, re-sampling, and re-quantization.

Problem Formulation

Different researchers discuss different techniques to protect the cloud server from internal attacks. Some researchers have implemented machine learning algorithms on datasets and discussed various techniques. Some researchers have discussed that spam messages have no statistical behavior. To prove this, they tried to train algorithms using different datasets. Some Authors worked on security modes, risks, and threats, in which they discussed the importance of the cloud's initial level of security. Some researchers have discussed that when the botnet ratio on a cloud server increases, the prevention of botnets decreases; to prove this, they used the deep learning technique convolutional neural network (CNN). However, no paper has experimentally proved how a spamming attack happens on a cloud server can be stopped, and the cloud server can be saved from such spamming.

In paper [27], a tool was developed to protect the cloud server from outside attacks, with the help of which the cloud server was protected from brute force and pattern matching attacks, and various techniques for preventing inside attacks were discussed. In this latest work, the current tool has been updated to protect the cloud server from spamming attacks by using Cloudflare and blocking the attacker's PC static and dynamic IP addresses through Cloudflare. Whenever an attacker attacks a cloud server, it uses static or dynamic IP addresses that Cloudflare will block. After that, when spamming is done several times, the attacker's IP address will be tracked by KNN classification. KNN classification will find the nearest neighbor and locate the attacker.

3 Proposed Methodology

3.1 Network Architecture

This article has designed architecture to protect the cloud from the inside. This architecture consists of two countries, WN1 and WN2, and each country consists of different cities. Cities are represented by C1, C2, . . . ,CN. Public Class-A IP addresses have been used for W1 and W2, while Private Class-C IP addresses have been used for different cities. The IP address of each city will be different from the other city. When a user accesses the cloud server, that user will be allocated a dynamic or static address.

In this paper, WN1 country has a spammer whose target is to destroy and misuse the cloud server data, as shown in Fig. 2. The attacker will send two spam messages one by one using the IP address of the city C2 of WN1 country. This spam aims to gain full access to the Peer to Peer network. This spam will be sent to the peer-to-peer network via a virtual switch. The Virtual Switch will act as an interface that will connect all WN1 and WN2 computers and devices to different servers and exchange data. After that, the attacker will attack the client-server network via one more IP address. The spamming attack on the client-server network is to manipulate the cloud server's data and gain access to the cloud server.

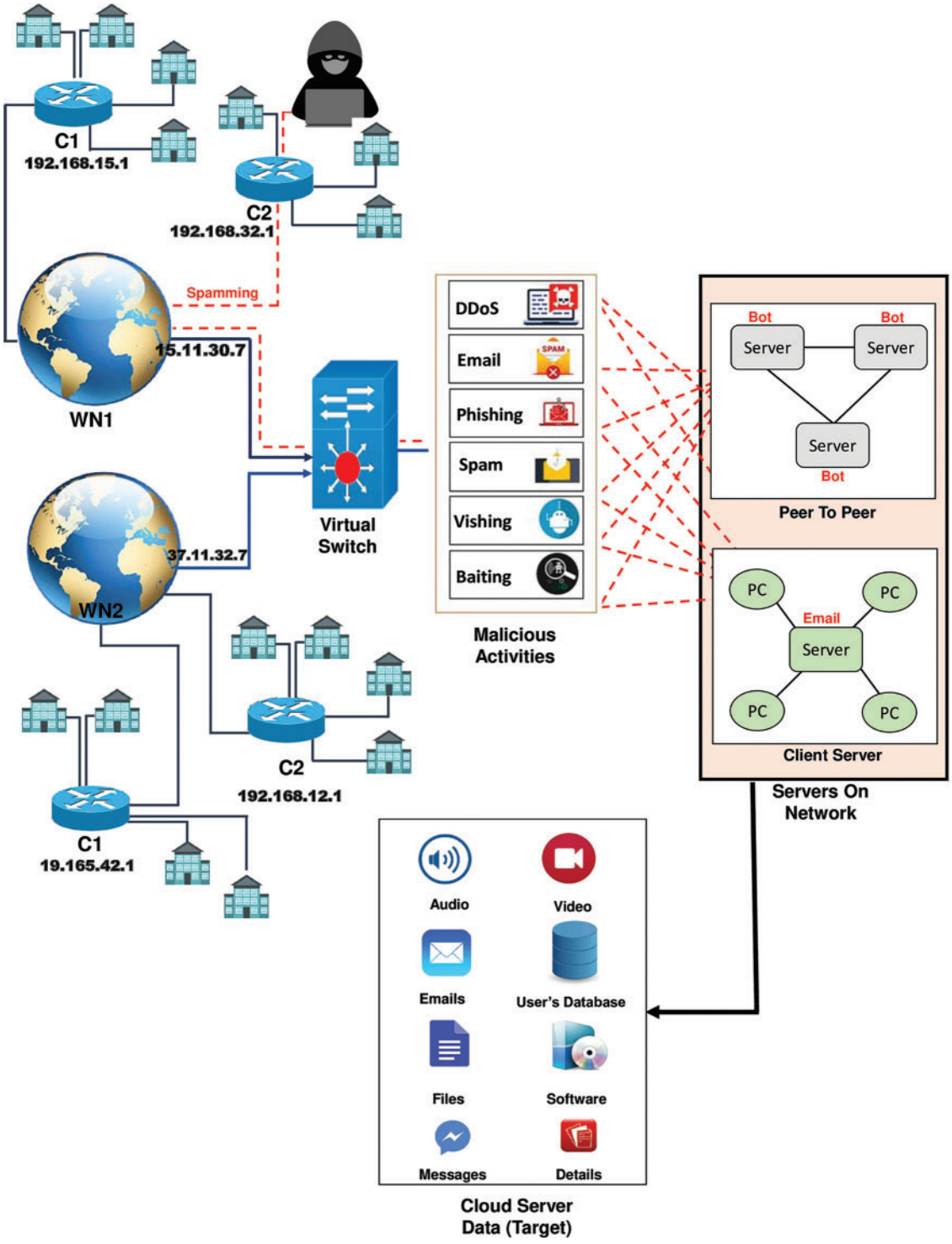

Figure 2: Network architecture

3.2 WN1 and WN2

WN1 and Country-2 represent Country-1 is represented by WN2. WN1 and WN2 consist of different cities. The cities of WN1 and WN2 are represented by C1, C2. . . . . ,CN. Each city has a different IP address than another city. Public IP addresses have been used for WN1 and WN2 countries, while private IP addresses have been used for WN1 and WN2 cities. The IP address of the WN1 country is 15.11.30.7 whereas the IP address of the WN2 country is 37.11.32.7.

3.3 Virtual Switch

The virtual switch will act as an interface. Whenever a user tries to access the cloud server, whether from a country or a city, the user will be connected to a virtual switch. Peer-to-Peer networks and Client-Server networks will be connected to Virtual Switch as shown in Fig. 2.

3.4 Servers on Network

The architecture of this paper consists of two types of networks. One is a peer-to-peer network, and the other is a client-server network. Complete data will be transmitted between all servers on a peer-to-peer network, while clients will only access server data while remaining on the client-server network. In Peer-to-Peer, all servers will have the same status whereas, in Client-Server Network, the Server will have all accessibility, and different PC's only accessing the data.

3.5 Prevention from Spamming Attacks Through Cloudflare

Whenever an attacker spams on a cloud server, a few spamming messages can be blocked easily, but it will be difficult to block every spam message when spamming is repeated. This paper uses Cloudflare to solve this problem. In addition to blocking spamming messages, if the attacker's IP address is blocked, spamming attacks are greatly reduced. Whenever an attacker spam on a cloud server, the attacker uses two different types of IP addresses. One is the static IP address and the other is the dynamic IP address. If the attacker spams through the static IP address, that IP address can be permanently blocked, but it is difficult to block the dynamic IP address if the attacker attacks through a dynamic IP address.

Some rules have been designed for dynamic and static IP addresses. When an attacker sends spam for, the first time it will be considered a dynamic IP address, and this IP address and spam message will be blocked for 2 h. When the blocked IP address is unblocked after 2 h and the attacker re-spams using the same IP address, the IP address will be permanently blocked along with the spam messages. In Fig. 3, the attacker will carry out various attacks from the WN1 country. According to the rules, Cloudflare will temporarily or permanently block this spam IP address when different spam is sent to different servers.

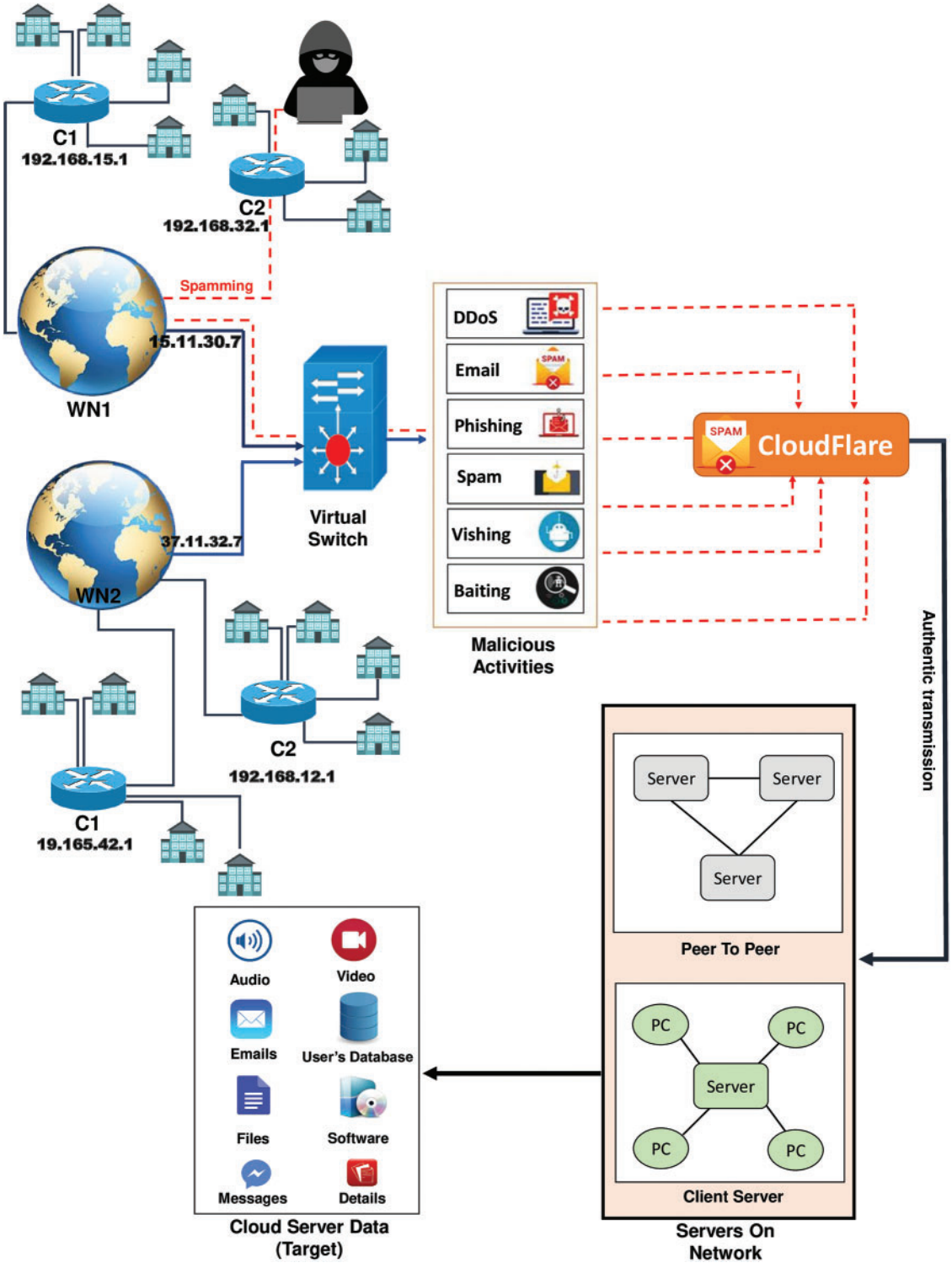

Figure 3: Prevention from spamming attacks through Cloudflare

4 Experiments

4.1 Spamming Attacks on Cloud Servers

The attacker carried out various attacks to misuse the cloud server and slow down its performance, in which first of all attacker connected the PC to the city (C2) of the country (WN1) and sent spam on the peer-to-peer network, as shown in Fig. 4.

```
wna --LD -e\lib\etc\users\Snbpy
Running --WN-mode
     ----Initializing System Files====--
Initializing ifup-hlip files!
Initializing ifup-SYS files!
Initializing Config.lib files!
Initializing Preprocessor!
[root@server ']# cs-e\lib\etc\sysconfig network.lib
[root@server ']# cs-e\lib\etc\sysconfig\system' ? y
PortCon  'FTP_PORT' defined: [20]
PortCon 'SHELL_PORTS' defined: [15:82 79:655192]
PortCon 'ORACLE_PORTS' defined: [1521]
Packets Limit: 256
                     Loading Files         82%[=============     ] 63kB/s


root@zpx-login: m_nadeem90
[m_nadeem90]@zpx-password: ******
[Port]-zpx: 3277
[SYSTEM]2zpx-show:

[UNKNOWN] --status | inet4 ::1/24 scope host
[default 15.11.30.7 dev enp0s3 proto static <metric 100>
ping from 192.168.14.7 [-h] [systemmd-UNKNOWN IP]| {invalid_lnk/loopback}]


                --== W  A  R  N  I  N  G ==--
                P R O E C T I O N  R E Q U I R E D
INFILTERATION ALERT
Your computer is being attacked by an internet virus
It could be a password-stealing attack, a trojran-dropper or similar
DETAILES
Attack from: 111.208.129.201, port: 46264
Attacked port: 20886
Threat: BankerFox.A
Do you want to block this attacks?

       Yes              No
     -------          ------
[SYSTEM]:>
```

Figure 4: First spam on peer to peer network from 192.168.14.7

When an attacker sent spam to a peer-to-peer network, the spam affected the entire network. This spam used a phishing technique to gain accessibility to the network where the attacker displayed a warning message. In this warning message, the attacker showed that your network has been attacked by the IP address 111.208.129.201 and sent a threat. The attacker then asked to block the attack. If the attacker's offer will be accepted, then with the help of this spam the attacker will gain access to the peer-to-peer network and perform spamming activities on the entire network. When the attacker's offer will not be accepted, the attacker will send a new boot as shown in Fig. 5.

In Fig. 5, the attacker sends a new bot to the peer-to-peer server, introducing a freeware tool to prevent malware attacks. The attacker attacks twice from the same IPaddress.

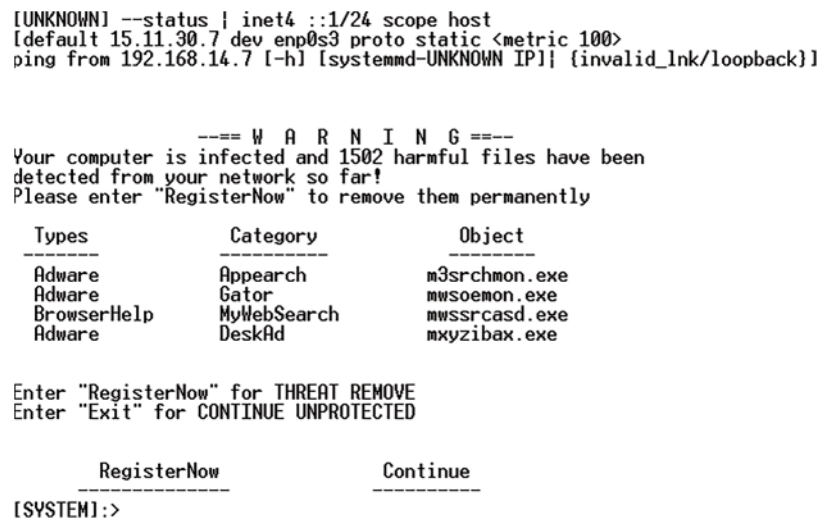

Figure 5: Second spam on peer to peer network from 192.168.14.7

In Fig. 6, the attacker sends a spam email on the client-server network from IP address 192.168.32.3, which stated that his email address is selected to receive 500 000.00 and is asked to sign up an account on the server-PC. The purpose of "Register Now" is to get the details of the server PC and destroy all the data of the server computer. When the user will not accept the offer, the attacker will repeatedly send offers and will continue to do so until the offer is accepted. It is very difficult to prevent the cloud server from such attacks. The best way to prevent cloud servers from such attacks is Cloudflare.

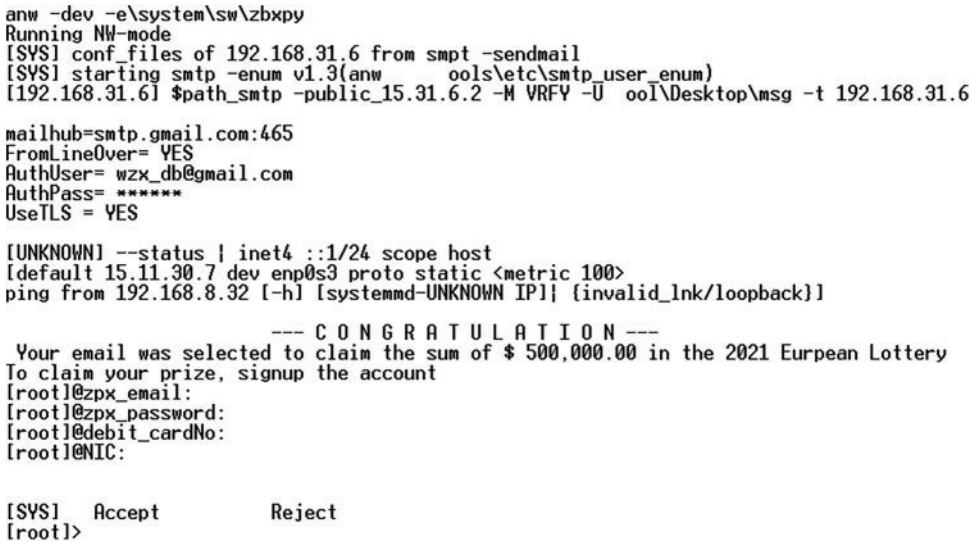

Figure 6: Spam message on client-server network from 192.168.32.3

4.2 Prevention from Spamming Attacks through Cloudflare

Whenever a user is login to a cloud server or performs an activity, the user has been assigned an IP address, whether the user is an authentic user or an attacker. Whenever there is spamming activity on the cloud server, it is through two IP addresses. One static IP address and the other dynamic up address.

4.2.1 Prevention from Static and Dynamic IP Address

Whenever an attacker spams on a cloud server, he does through an IP address. Cloudflare has been used to prevent such activities. Cloudflare has blocked two types of internal attacks. The first is that whenever an attacker spams through an IP address for the first time, it will be considered a dynamic IP address and blocked for two hours. The second is that, If the attacker spams again using the same IP address, the IP address will be considered static and blocked permanently. The reason for considering the IP address to be dynamic is that maybe the IP address is dynamic and the next time it is assigned to another user. Blocking an IP address will not affect a PC or server nor will server performance be slow. In Fig. 7, the attacker sent spam, and then this IP address is blocked for two hours. But again, sending spam from the same IP address, that IP address has been blocked permanently.

```
root@zpx-login: m_nadeem90
[m_nadeem90]@zpx-password: ******
[Port]-zpx: 3277
[SYSTEM]2zpx-show:


[?] 01 Unknown messages Detected
[SUCCESS]# Service {www.terra-1.indriveapp.ua}>>Blocked!
[Status]~ message_from root@tecmint}#(Sun Dec 12 9 13:29:15 2021):
[400]~ Service_FAILED>>[default 15.11.30.7 dev enp0s3 proto static <metric 100>!
ping from 192.168.14.7 [-h] [systemmd-UNKNOWN IP]¦ {invalid_lnk/loopback}]
[Account_INFO]# Blocked
[Duration]~02_hours

[?] 01 Unknown messages Detected
[SUCCESS]# Service {api.mstv.yandex.com}>>Blocked!
[Status]! message_from root@tecmint}#(Sun Dec 12 10 05:12:54 2021):
[400]! Service_FAILED>>[default 15.11.30.7 dev enp0s3 proto static <metric 100>!
ping from 192.168.14.7 [-h] [systemmd-UNKNOWN IP]¦ {invalid_lnk/loopback}]
[Account_INFO]# <Permanent_Blocked>
```

Figure 7: Dynamic IP address blocking

The second way is to restrict Cloudflare instead of blocking the IP address. If the spammer sends any harmful activity to the cloud server, that action will be destroyed, and only authentic transmissions will be on cloud servers as shown in Fig. 8.

```
root@zpx-login: syeda.wajia786
[syeda.wajia786]@zpx-password: *****
[Port]-zpx: 3277
[SYSTEM]2zpx-show:


[Detected] 02 threats detected

[SYSTEM]:>
```

Figure 8: Threat detection

4.2.2 Cloudflare Prevention Algorithm

Some rules have been applied to test the performance of Cloudflare, and four variables named *A, B, C* and *D* have been used. "*A*" variable represents the user's action or user activities. Variable "*B*"

represents the effect of the servers. The "*C*" variable indicates the performance of Cloudflare. The "*D*" variable indicates whether access to the cloud server is possible or not.

Representation of variables

- If $A = 0$, it means that the user is performing unauthorized activities, whereas $A = 1$ means that the user is performing authentic activities.
- If $B = 0$ then it means that the server has been attacked whereas $B = 1$ means that the server has not been attacked.
- If C gets a value of 0 from A and B, it means that Cloudflare has stopped the spamming activity and stopped this process. If C gets a value of 1 from A and B, it means that Cloudflare carried this process to D.
- If D = 0, it means that C does not send the action to D. If D = 1 means C has forwarded the process and gives the user access to the cloud server.

Conditions

- If $A = 0 \rightarrow B \simeq 0$.
- If $A = 1 \rightarrow B \simeq 1$.
- $C \in A * B_{\cdot}^{\cdot} D \in C$

$X = 0$ means that the spammer tried to attack the cloud server, but the attacks did not affect the cloud server's data and network performance. $X = 1$ means authentic inside activities are performed on the cloud server without intrusions as shown in Tab. 1.

Table 1: Result of resources accessibility by cloudflare

User response	Server response	Cloudflare response	Resources accessibility	Results
A	B	$C \in AB$	$D \in C$	$X = C \wedge D$
0	0	0	0	0
1	1	1	1	1

The mathematical expression of f(x) is as follow

$$F(x) = \Leftrightarrow C \wedge D \simeq 1 \rightarrow \top (X) \tag{1}$$

4.3 Identification of Attacker's Location via KNN Classification

KNN classification has been used to detect an attack within a cloud server. Whenever an attacker attacks a cloud server, it connects to any IP address. Static IP addresses can be permanently blocked, but dynamic IP addresses are difficult to block permanently, but it can be known from which city and which country the attack took place.

Firstly, the default gateway has been detected with the help of the attacker's IP address *192.168.14.7*, as shown in Fig. 9. Gateway of IP address *192.168.14.7* has been obtained *15.11.30.7*. *15.11.30.7* is the IP address of WN1. After that, all the IP addresses associated with the WN1 country have been accessed as shown in Fig. 10.

```
nw@zpx-login:  SYSTEM
[SYSTEM]@zpx-password:  ******
[PORT]-zpx-:  3277
[SYSTEM]@zpx-show: ipconfigdet_192.168.14.7

root@zpx_DATABASE: Pinging 192.168.14.7 with 32 bytes of data:
PORT  STATE SERVICE
Network Distannce: 2 hop

Please Wait...
root@zpx_DATABASE:192.168.14.7 is connected...

Ping Stistics for 192.168.14.7
Packets: Sent = 4, Recieved = 4, Lost = 0

Ethernet adapter Ethernet:
        Media Status.....................................: Connected
        Connection-specific DNS suffix ..................: PTCL-BB


Ethernet LAN adapter Wi-Fi:
        Media Status.....................................: Disconnected
        Connection-specific DNS suffix ..................: Disable


Ethernet adapter Detail:
        IPV4 address.....................................: 192.168.14.7
        Port Number .....................................: 3277
        Link-local IPV6 address .........................: 2122:dAa2:1020::a56x:953f
        Subnet Mask .....................................: 255.255.255.0
        Default Gateway .................................: 15.11.30.7
```

Figure 9: Detail of IP address 192.168.14.7

```
[SYSTEM]@zpx-show: ipdispall
```

Organizations	Protocols	Status	DNS-Suffix	Location
Dozti	192.168.15.1	Connected	Dlink	Sydney
Lonicy	192.168.41.27	Connected	vlink_n3305	Adelaide
Gozzby	192.168.8.32	Connected	Netgear C300	Canberra
Yiglo	192.168.11.41	Connected	Linksys WR30	Newcastle
Vorbax	192.168.32.1	Connected	Tenda	Perth
Anetly	192.168.47.25	Connected	Dlink	Melbourne
Daniry	192.168.39.22	Connected	DIR-X6060	Hobart
Lorofy	192.168.16.46	Connected	Dlink	Brisbane

Figure 10: Status of all cities of WN1

To find the attacking area, all the Network-IDs have been identified, in which the IP addresses of all cities of WN1 country are listed in Tab. 2. Network-ID has been then figured out. To find the network id the network portion has been completely on and the host portion has been completely off. After that, the mathematical expression of KNN has been used and different results are shown. Different IP addresses of country WN1 are shown in Tab. 2.

$$f(x) = \sqrt{x_{1p} - x_{1a})^2} \tag{2}$$

First, the value of K has been assumed to be $K = 3$. $K = 3$ means to get the three closest IP addresses closest to the attacker's IP address, as shown in Fig. 11. The last octet of the network portion of these IP addresses will be used in the formula, and different results will be obtained. X1p means predictive value while X1a means actual value. The predicted value has been obtained from the spammer network ID 192.168.14.7, while the actual value has been obtained from the last octet of the nearest neighbor's network ID.

Table 2: IP addresses of WN1 country

WN1 Country			
Cities IP addresses	Network ID	Nearest neighbors	Results of K
192.168.15.1	192.168.*15*.0	✓	$=\sqrt{13-15)^2}$ $=2$
192.168.32.1	192.168.*32*.0	✗	✗
192.168.41.2	192.168.*41*.0	✗	✗
192.168.8.32	192.168.*8*.0	✓	$=\sqrt{8-15)^2}$ $=7$
192.168.11.41	192.168.*11*.0	✓	$=\sqrt{11-15)^2}$ $=4$
192.168.47.25	192.168.*47*.0	✗	✗

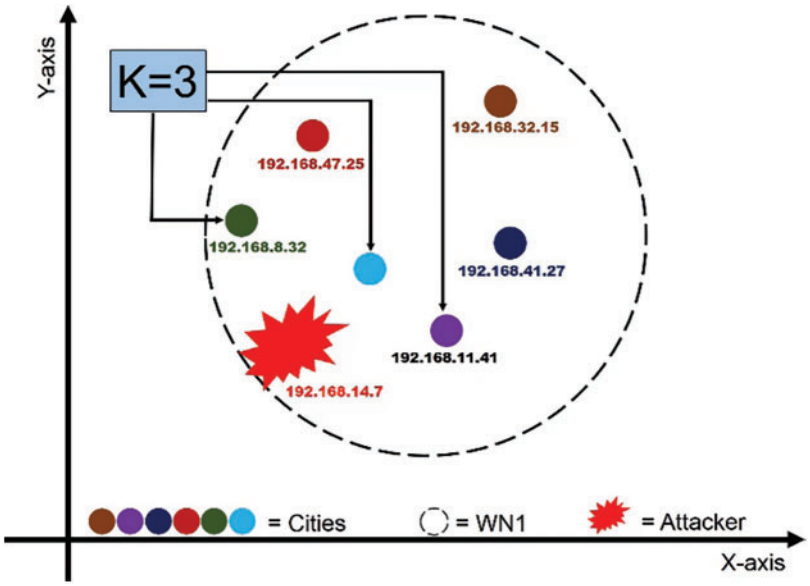

Figure 11: Nearest neighbors of IP address 192.168.14.7

After getting different results as shown in Fig. 11, the smallest value of "K" got K = 2. This means that the IP address 192.168.14.7 is the closest to 192.168.15.1. The IP address of K = 2 is 192.168.15.1, which represents C1 City, then it means that the attacker is closest to City C1 and belongs to WN1 country. The dynamic IP address cannot fully determine the location of any attacker, but it is possible to find out from which city and country the attack took place, as revealed in this paper.

4.4 Comparative Analysis

Different researchers have designed different algorithms to secure the cloud server and applied these algorithms in other machine learning techniques. Some researchers surveyed various papers and discussed different methods for protecting the cloud from the inside as shown in Tab. 3.

Table 3: Comparative analysis

Sr#	1	2	3	4	5	Proposed work
Paper Name	Cloud computing security challenges	Toward a deep learning-based intrusion detection system for IoT against botnet attacks	Spam-detection with comparative analysis and spamming words extractions	Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system	An efficient network intrusion detection and classification system	
Year	2020	2021	2021	2021	2022	
Reference #	[24]	[25]	[26]	[27]	[28]	
Problem statement	Lack of initial level of cloud security	Prevention from botnet attacks	distinguished spam messages from normal message	Prevent the cloud servers from various attacks	Identification of threats for system	Prevent the cloud server from spamming attacks
Proposed Solution	Various tactics to secure the cloud infrastructure	Baptized botids" technique based on the deep learning convolutional neural network	Identify the repeated keywords and implement four datasets onto two deep learning algorithms	Implemented cloud Shell to protect against various attacks and discussed cloudflare to protect against DDoS attacks	AdaBoost-based approach Used UNSW-NB dataset	Implement cloudflare to protect from spamming and identified the attacker location through KNN

In paper [24], the researchers argued that the main reason for the cloud attack is the lack of essential protection. As long as the cloud server is not provided with basic security, the attack rate

cannot be reduced, for which discussed different techniques of cloud server infrastructure. However, no algorithm or method has been implemented in this paper to provide security to the cloud internally or externally. In article [25], Researchers have discussed that as the number of botnet attacks on a cloud server increases, Botnet attacks reduce the ability of algorithms used to protect cloud servers, causing every device to turn into a zombie. The Baptized BotIDS technique was developed to address this issue and implemented on the Deep Learning Conventional Neural Network. The problem with this paper is that if the attacker spam through a static or dynamic IP address, the spam message can be stopped, but the attacker cannot. In the paper [26], Researchers wanted to distinguish regular messages from spam messages by identifying keywords frequently used in spam messages. For which they implemented four data sets on two deep learning algorithms. The problem with this paper is that keyword identification is a time-consuming process. If an attacker tries to attack using different IP addresses, then the keyword identification of each attacker becomes more challenging to detect. In the paper [27], a tool was developed to protect the cloud server from internal and external attacks, using a variety of techniques to protect against external attacks such as pattern matching and brute force and to protect against internal attacks such as DDoS, only the Cloudflare technique had been discussed, but no method has been implemented in this paper to block the attacker static or dynamic IP addresses via Cloudflare, Nor has any way discussed to identify the attacker's attacking location from which country or city the attacker was attacking the cloud server.

Various researchers have designed different algorithms for securing the cloud server to discuss how cloud servers can be protected from such attacks. However, none of the articles practically implemented these algorithms. If an attacker attacks a cloud server, "How can these algorithms detect such attacks, and how can the cloud server prevent these attacks"?

4.5 Novelty of Proposed Work

Whenever an attacker attacks the cloud server or tries to spam it, the spammer message and its IP addresses are blocked by Cloudflare, and only authorized activities are allowed on the cloud server. Whenever an attacker attempt spamming using a static or dynamic IP address key, KNN can be used to identify the attacker's location. With the help of KNN, the country and city of the attacker can be identified as done in this paper. Suppose an attacker attacks by static IP address, such IP address can be permanently blocked by Cloudflare but, whenever an attacker attacks via a dynamic IP address. In that case, such an IP address cannot be permanently blocked. If the dynamic IP address is permanently blocked, then this IP address cannot be used unless it is unblocked, which is a big problem. Suppose an attacker attacks an attacker using a dynamic IP address. In that case, KNN can be used to locate the attacker and stop the country or city's accessibility to the cloud for a specific time, as done in this article, which will significantly reduce the chances of spamming. A cloud server will only be secure when its internal and external components are secure. Cloud servers can only be secured from the inside if different security algorithms are applied at each stage. Whenever a user is given access to a cloud server, the user's limits must be set. The detection mechanism should be used when the user tries to exceed the limit or misuse the server, and the user's account should be permanently blocked.

5 Conclusion

After developing and testing the software, it has been concluded that if the cloud server is protected from attacks such as spamming, it can be protected from within. Internal attacks on the cloud are carried out to misuse cloud server users or destroy users' data. If the cloud is to be protected from the inside, IP-based prevention must be used with limited access to each IP address. Suppose an attacker

tries to carry out malicious activity toward the user. In that case, an algorithm should be designed to transmit only authentic packets. When a user tries to perform a malicious activity, such user and his interfering packet should be automatically removed from the cloud server. External attacks on the cloud server can be more easily prevented than internal attacks. Different algorithms and techniques can be designed to protect the cloud server from the outside, but it is very difficult to design algorithms to protect the cloud server from internal attacks. When each user is provided with a static IP address, this IP address can be permanently blocked at the same time due to misuse of the cloud server, but only when the user is working through dynamic IP addresses. Such IP addresses and attacks will be very difficult to detect. The best way to protect the cloud server from internal attacks is to use Cloudflare as described in this paper and use the KNN algorithm to determine the location of the attacker.

In the future, a hashed mechanism will be designed to secure the server data and cloud server, and a salting algorithm is implemented on hashing to secure the internal and external sides. In addition, an efficient tool will be developed to secure the cloud server from inside and outside and a comparison of the tool will be made with OSSEC and snort and discuss the efficiency of the best tool.

Author Contributions: M.N. Conceptualization and Methodology; A.A. Software, Writing—review & editing; S.R. Writing—review & editing; S.W.Z. Methodology; M.R. review; S.S. funding acquisition; and A.M. Editing.

Acknowledgement: We would like to thank Abasyn University for their resources and help throughout the development of this project and our time gaining the knowledge and tools we would need to succeed in the professional world.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Khandelwal, A. Dogra, K. Ganti, S. Purini and P. V. Reddy, "Pricing strategies of an oligopolist in federated cloud markets," *Journal of Cloud Computing*, vol. 10, no. 54, pp. 1–13, 2021.

[2] G. H. Lokesh and G. BoreGowda, "Phishing website detection based on effective machine learning approach," *Journal of Cyber Security Technology*, vol. 5, pp. 1–14, 2020.

[3] S. Liu, J. Wu and C. Long, "IoT meets blockchain: Parallel distributed architecture for data storage and sharing," in *2018 IEEE Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, pp. 1355–1360, 2018.

[4] Y. A. A. S. Aldeen, M. Salleh and M. A. Razzaque, "A survey paper on privacy issue in cloud computing," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 3, pp. 328–337, 2015.

[5] W. Ahmed, A. Rasool, A. R. Javed, T. Baker and Z. Jalil, "Cyber security in IoT-based cloud computing: A comprehensive survey," *Electronics*, vol. 11, no. 16, pp. 1–34, 2022.

[6] M. Gowda HR, M. V. Adithya, G. S. Prasad and S. Vinay, "Development of anti-phishing browser based on random forest and rule of extraction framework," *Cybersecurity*, vol. 3, no. 1, pp. 1–14, 2020.

[7] A. Altaher, "Phishing websites classification using hybrid SVM and KNN approach," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 90–95, 2017.

[8] A. J. Park, R. N. Quadari and H. H. Tsang, "Phishing website detection framework through web scraping and data mining," in *2017 8th IEEE Annual Inforation Technology, Electronics and Mobile Communication Conf. (IEMCON)*, Vancouver, BC, pp. 680–684, 2017.

[9] S. Saxena, A. Shrivastava and V. Birchha, "A proposal on phishing url classification for web security," *International Journal of Computer Applications*, vol. 178, no. 39, pp. 47–49, 2019.
[10] M. Zouina and B. Outtaj, "A novel lightweight url phishing detection system using SVM and similarity index," *Human-centric Computing and Information Sciences*, vol. 7, no. 1, pp. 1–13, 2017.
[11] Y. S. Rao, A. K. Keshri, B. K. Mishra and T. C. Pand, "Distributed denial of service attack on targeted resources in a computer network for critical infrastructure: A differential e-epidemic model," *Physica A: Statistical Mechanics and Its Applications*, vol. 540, no. 4, pp. 123240, 2019.
[12] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki,"Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no.3, pp. 2671–2701, 2019.
[13] S. T. Zargar, J. Joshi and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.
[14] Y. Gu, K. Li, Z. Guo and Y. Wang, "Semi-supervised k-means DDoS detection method using hybrid feature selection algorithm," *IEEE Access*, vol. 7, pp. 64351–64365, 2019.
[15] S. M. Abdulhamid, M. Shuaib and O. Osho, "Comparative analysis of classification algorithms for email spam detection," *International Journal of Computer Network and Information Security*, vol. 10, no. 1, pp. 60–67, 2018.
[16] C. Palanisamy, T. Kumaresan and S. Varalakshmi, "Combined techniques for detecting email spam using negative selection and particle swarm optimization," *International Journal of Advanced Research Trends in Engineering and Technology*, vol. 3, no. 2, pp. 1102–1106, 2016.
[17] S. Newman, "Under the radar: The danger of stealthy DDoS attacks," *Network Security*, vol. 2019, no. 2, pp. 18–19, 2019.
[18] R. Singh, A. Prasad, R. Moven and H. Samra, "Denial of service attack in wireless data network: A survey. devices for integrated circuit," in *Proc. of the 2017 Devices for Integrated Circuit (DevIC)*, Kalyani, India, pp. 23–24, March 2017.
[19] S. Chikhi and R. Chikh, "Clustered negative selection algorithm and fruit fly optimization foremail spam detection," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 143–152, 2019.
[20] X. Hu, B. Li, Y. Zhang, C. Zhou and H. Ma, "Detecting compromised email accounts from the perspective of graph topology," in *Proc. of the 11th Int. Conf. on Future Internet Technologies*, Nanjing, China, pp. 76–82, 2016.
[21] S. Dhavale, "C-Asft: Convolutional neural networksbased anti-spam filtering," in *Proc. of Int. Conf. on Computational Science and Applications*, Pune, India, pp. 49–55, 2020.
[22] S. S. Roy, A. Sinha, R. Roy, C. Barna and P. Samui, "Spam email detection using deep support vector machine, support vector machine and artificial neural network," in *Int. Workshop Soft Computing Applications*, Arad, Romania, Springer, pp. 162–174, 2016.
[23] C. Wang, Q. Li, T. Ren, X. Wang and G. Guo, "High efficiency spam filtering: A manifold learning based approach," *Mathematical Problems in Engineering*, vol. 2021, pp. 1–7, 2021.
[24] N. R. Tadapaneni, "Cloud computing security challenges," *Ssrn Electronic Journal*, vol. 7, no. 6, pp. 1–6, 2020.
[25] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui and H. E. Fadili, "Toward a deep learning-based intrusion detection system for IoT against botnet attacks," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 10, no. 1, pp. 110–120, 2021.
[26] M. K. Islam, M. A. Amin, M. R. Islam, M. N. I. Mahbub, M. I. H. Showrov *et al.,* "Spam-detection with comparative analysis and spamming words extractions," in *2021 9th Int. Conf. on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, pp. 1–9, 2021.
[27] M. Nadeem, A. Arshad, S. Riaz, S. S. Band and A. Mosavi, "Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system," *IEEE Access*, vol. 9, pp. 152300–152309, 2021.

[28] I. Ahmad, Q. Haq, M. Imran, M. Alassafi and R. A. Ghamdi, "An efficient network intrusion detection and classification system," *Mathematics*, vol. 10, no. 3, pp. 530, 2022.
[29] X. R. Zhang, W. F. Zhang, W. Sun, X. M. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science & Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.
[30] R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.