IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 13, 2021, accepted November 4, 2021, date of publication November 8, 2021,
date of current version November 18, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3126535

Intercept the Cloud Network From Brute Force and DDoS Attacks via Intrusion Detection and Prevention System

MUHAMMAD NADEEM[1], ALI ARSHAD[2], SAMAN RIAZ[3], SHAHAB S. BAND[4], (Senior Member, IEEE), AND AMIR MOSAVI[5,6]

[1]Department of Computing, Abasyn University, Islamabad 75660, Pakistan
[2]Department of Computer Science, Institute of Space and Technology, Islamabad 44000, Pakistan
[3]Department of Computer Science, National University of Technology, Islamabad 44000, Pakistan
[4]Future Technology Research Center, National Yunlin University of Science and Technology, Douliu, Yunlin 64002, Taiwan
[5]Faculty of Civil Engineering, Technische Universitat Dresden, 01069 Dresden, Germany
[6]John von Neumann Faculty of Informatics, Obuda University, 1034 Budapest, Hungary

Corresponding authors: Ali Arshad (alli.arshad@gmail.com), Shahab S. Band (shamshirbands@yuntech.edu.tw), and Amir Mosavi (amir.mosavi@mailbox.tu-dresden.de)

This work was supported by the Open Access Funding by the Publication Fund of the TU Dresden.

ABSTRACT Cloud computing is considered to be the best technique for storing data online instead of using a hard drive. It includes three different types of computing services that are provided to remote users via the Internet. Cloud computing offers its end users a variety of options, such as cost savings, access to online resources and performance, but as the number of users in cloud computing grows, so does the likelihood of an attack. Various researchers have researched and provided many solutions to prevent these attacks. One of the best ways to detect an attack is through an Intrusion Detection System. This article will develop an efficient framework in which will use and discuss various security solutions for a network. Every device on the network will be attacked and the attack rate of the entire network will be monitored. After that, various solutions will be provided to protect the cloud server from attacks. Different principles will be used at the end of the article to test the accuracy of the results and from each conclusion it will be concluded to what extent the results of this paper are better than others.

INDEX TERMS Intrusion detection system, network based intrusion detection system, host based intrusion detection system, spam, DDoS, Bot, cloud security.

I. INTRODUCTION

Cloud computing is becoming a necessity in the world right now [1]. Each company is moving to the cloud to run its business. Cloud computing offers many services free of cost to its users, including storing and accessing data from anywhere in the world. Cloud computing and distributed systems are two similar devices because, In a distributed system, data is distributed in different places and retrieved from anywhere in the world. In contrast, in cloud computing, all information is stored on the Internet and can be accessed remotely from anywhere.

Client servers computing were used before the invention of cloud computing. Client server is a model in which all the data on the server can be retrieved only by clients connected to that server, while the server can use and change resources. If a clients want to access specific data from the server, they can easily connect their PC to the server-PC key and access the resources. Cloud computing was developed based on the concept of distributed systems and client-server systems.

Cloud users are offered three cloud computing models: private model, public model, and hybrid model. The public model is a free model that is freely accessible from any part of the world. There is always a third party that runs and operates the cloud servers. The private cloud is a much more reliable and safe cloud because this cloud is designed for one organization only and can be accessed within the organization. Many organizations have moved their business from public cloud to private cloud. Hybrid cloud is the third model of cloud computing that has the best features of both clouds.

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

Hybrid cloud connects at least one private cloud and at least one public cloud with each other and provides protection, flexibility, and capabilities to any organization.

Cloud computing requires two types of security to protect the cloud from malware [2]. One is data security, and the other is network security. Many threats in the cloud data center are trying to damage the cloud or try to stole or snatch the data from the cloud. Various researchers have shown that if an intrusion detection system is installed on every cloud device and every security measure is used on the device, then there will be very little chance of attacks. Many intruders design various attacking algorithms, encryption, and decryption techniques to snatch data from cloud servers. This invasive technique can destroy the data of the cloud server, and all the data can be corrupt. A secure architecture can preserve the cloud server.

When storing various information in a cloud server, security is also required after storing the data. A cloud can only be safe if it has a set of implementations, methods, and techniques. Different researchers have designed different algorithms, procedures, and strategies to secure the cloud. The best of these is Intrusion Detection System. An Intrusion Detection System (IDS) is a mechanism that controls doubtful actions and policy violations from a network [3]. The Intrusion Detection System can detect malware from the cloud. It issues an alert to the cloud administrator when an intruder attempts to attack the cloud data center. The most significant advantage of the Intrusion Detection System (IDS) is that it monitors the arriving activities in the network and sees whether these activities are valid or invalid. Some Intrusion Detection Systems are so capable that they respond as soon as malware is discovered. There are vast arrays of Intrusion Detection System (IDS) available in antivirus, detecting intrusions from cloud servers. The most common Intrusion Detection System are [4]

- Network Based Intrusion Detection System (NIDS)
- Host Based Intrusion Detection System (HIDS)
- Signature Based Intrusion Detection System (SIDS)
- Anomaly Based Intrusion Detection System (AIDS)

NIDS is used to detect interference from the network. It is also used to monitor all devices connected to the network. Like NIDS, HIDS also plays an essential role in the network. HIDS is used to detect and monitor suspect actions on the host PCs or devices. NIDS works on network devices, while HIDS works on host PCs. Anomaly-Based IDS and Signature-Based IDS are the subsets of the Intrusion Detection System. In signature-based IDS, a signature is used. Its function is to monitor the activity on the network, whether it is authentic or non-authentic. Anomaly-Based depend on system behavior. When an attacker tries to turn a normal behavior of the system into abnormal behavior, an anomalous detection system detects it.

This article will design and work on the architecture to install a separate router in each country and use a unique port number for each router to distort the country. We will then associate IDS with each country and see how we can detect if someone attacks the router. Finally, we will apply some rules and conclude that if an effective algorithm is designed to detect an attack from the cloud, what is the probability of detecting an attack from the cloud.

The rest of the papers are as follows. Section II will explore recent developments in introductory research. Section III will present our new proposed Methodology. In Section IV, we will represent the experimental results, and Section V will be the conclusion of the article

II. RELATED WORK

Narendra *et al.* worked on cloud security challenges and discusses how the cloud can be protect from the basic level [1]. In this paper, authors discussed several attacks, threats, and models on the cloud server. According to the authors, the cloud stores and manages all types of data, but there are a number of risks involved when storing data. The biggest problem with cloud computing is cloud security and its attacks. Each technology requires two stages. One stage leads to challenges and the other stage leads to prosperity. Similarly, in cloud computing, one phase provides benefits, and the other phase leads the cloud to challenges. Challenges includes inside attacks, lack of support and standardization, malware threats, etc. The article concludes with a key security issue, discusses the reasons for the privacy breach and also discussed some of the dangers of destroying clouds.

According to Jyoti Snehi [2], the Intrusion Detection System is a device that connects to the network and monitors suspicious activity within the network and notifies the network administrator after a breakdown. If a network engages in malicious activity, it could potentially destroy important information, such as user loyalty and data breaches. Whenever an organization uploads its data to the cloud server, it needs to save the data from internal and external threats such as password cracking. Anti-malware and firewall software alone is not sufficient to protect the entire network or provide protection alone. This article discusses the different datasets used in different articles and concluded that interference across the entire network could be detected using IDS.

Aryachandra designed the architecture based on a network [3] where the architecture was implemented on an efficient tool name snort. This architecture used two cloud servers and two ports for interference. Port name are VMBR1 and VMBR2 whereas cloud server names are cloud server-1 and cloud server-2. In this article, the author uses Intrusion Detection System (IDS) in three different places at three different times. In the first time, Intrusion Detection System (IDS) was placed outside of the cloud server. In the second time, Intrusion Detection System (IDS) was placed inside of the cloud server. In the third time, Intrusion Detection System (IDS) was placed both side in the cloud servers. After the attack on the network, three truth tables were set up to indicate the possibility of an attack. At the end of the article, Snort examined the effect of RAM and CPU during execution

and found that RAM affects only 0.25% during execution. In contrast, CPU has no effect during execution.

Gassais *et al.* worked on Intrusion Detection techniques and proposed an automated host-based framework [5]. This article connects user and core spaces and uses machine learning methods to detect Intrusion from smart devices. One of these is the tracking technique that automatically deals with devices and processes data by using machine learning algorithms and produced alert. One of the many algorithms used in this article is the deep learning algorithm, which can detect interruption. The author tested this solution inside a realistic home automation system with real risks and demonstrated how it can be adapted to various devices and explain how this solution works well, taking advantages of its host-oriented approach.

As data storage on the cloud server increases, so does the attack rate on the cloud server also increasing [6]. Cyber security is becoming the biggest problem right now. Failure to prevent the intrusion can damaged the reputation of security services. Jang Jacquard *et al.*, reviewed various Intrusion Detection techniques. Two of them are the Signature-Based IDS and the Anomaly Based IDS. In addition, some data resource techniques were used for the cloud. At the end, the author draws conclusions from recent papers and seeks to find innovative models for improving AIDS performance as a solution to Intrusion Detection System (IDS) issues.

Mehrnaz Mazini uses artificial bee colony technique for Anomaly based IDS [7] and develops a hybrid method and detects huge exposure charge with cheap definite charge using AdaBoost algorithm. Several features were selected with the help of Artificial Bay-Colony. While features are classified and tested using the Ada Boost algorithm. The meta-algorithm was used in the Ada Boost algorithm. It is related to the accuracy of the advanced method to organizing various attack groups. At the end of the paper, optimized the problem of Intrusion Detection System (IDS) by using Artificial Bee-colony meta-algorithm.

Vishal and Vasudha reviewed various papers and discussed that there are many possible causes for DOS attacks [8]. DOS attacks can be on cloud servers, websites, layers of OSI model, etc. According to authors, DOS attack fills servers with malicious traffic that completely blocks the website or provides incomplete resources to end users while DDoS uses various machines or computers and fill the machine with malicious traffic. DDOS Attack sends an unlimited number of requests to the server using illegal IP addresses and these addresses are difficult to locate. DDOS attack sends an unlimited number of requests to the server using illegal IP addresses and these addresses are difficult to locate. After reviewed, authors worked on OSI model and discussed all possible attacks on each layer of the OSI model, obtained from various papers. Finally, concluded that the accuracy of the Random Forest and Cat Boost algorithms is very high that is 99.99%.

Many researchers have done research to make the cloud safer. Different algorithms designed in different research. Many architectural constructions were done to keep the architects safe. Some researchers surveyed different papers and demonstrated better detection techniques. In paper [8], The authors reviewed several papers and collected different types of DDOS attacks that occurred in different papers after that placed different attacks on each layer of the OSI model, and looked at which DDoS attack can possible on which layer but this article does not show any method to prevent the cloud from being attacked by DDoS, nor is there any discussion on DDoS attack detection techniques. This article will design a network topology in which DDoS attacks will be carried out inside the cloud server and Brute force and pattern matching attacks will be carried out outside the cloud server. HIDS will be used to protect the cloud from pattern matching attacks, while some brute force prevention methods will be discussed to protect the cloud server from brute force attacks. Similarly, the cloudflare technique will be used to prevent from DDoS attacks. After that, some mathematical rules will be applied to all the results and conclusions will be drawn based on these rules.

III. PROPOSED METHODOLOGY

A. ARCHITECTURE

In this paper, we will develop a cloud that will work like a real-time cloud in which we will use three routers (R1. R2 and URP), shown in Fig 1. We will assign a separate port number to each router. We will assign port number 5162 to the URP router and port number 5745 to cloud server. Similarly, we will assign port number 3295 to router R1 and port number 7635 to router R2. The URP router will act as an interface, and all the routers data will go to the cloud server through URP. We will rename the URP router as Business Layer because routers and PCs from all countries will use this router to connect to the cloud server. We used two routers for two different countries and two different port numbers for each country. The reason for using a separate port number for each country is that each country uses a unique address and communicates with the entire network using its own port number.

B. SUBNETTING

After designing an architecture, we will assign a unique IP address to each router using subnetting, shown in Figure 1. We use subnetting because we can provide an up-to-date address to each router like a real-time cloud. Instead of giving a separate IP address to each router, we will take an IP address and divide it into different IP addresses by using subnetting. If the PC wants to connect to its router, the client will receive a Class-C IP address. We will assign a public IP address to Router (R1 and R2), URP, and Cloud server while assigning a private IP name to Router R1 and Router R2 PCs.

First of all, we will subnetting so that we will take the class-A IP address 13.62.5.3, then we will create subnets according to the network. We will use a formula 2n-2 to make subnets. After the calculation, we will get four different

TABLE 1. Subnetting.

Subnets	Network-ID	Broadcast-ID	Subnet Mask
Subnet-1	13.0.0.0	13.63.0.0	255.192.0.0
Subnet-1	13.64.0.0	13.127.0.0	255.192.0.0
Subnet-1	13.128.0.0	13.191.0.0	255.192.0.0
Subnet-1	13.192.0.0	13.255.0.0	255.192.0.0

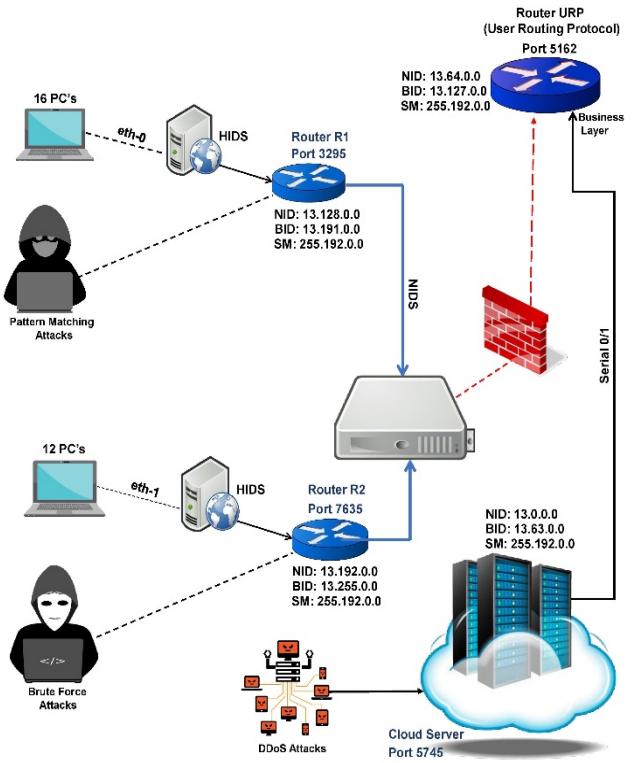

FIGURE 1. IP addressing of cloud computing.

subsets, including Network ID, Broadcast ID, and Subnet Mask.

C. ROUTER R1

We will assign port number 3295 to Router R1. Our procedure for Router R1 will be to first enter the user's User-ID and password, and then we will use the term "Signature" for verification purposes. The job of the signature will be to check the authenticity and inauthenticity of the incoming packets. If the incoming packets are authentic, the user will go to the second step of verification. The second step will be the port number that will show the country router. We will create three admin users in this router. We will provide each user with a unique user ID and password, and when the user clears step 1 verification, the user must verify step 2.

If the user does not clear the step 1 verification, the signature will not allow the user to enter step 2. When the user confirms step-1 and enters the second step, HIDS will check all the incoming keys of step 1 and step-2 along with the existing keys. If all keys match the existing keys, it means that it is an authorized user and will provide admin authority. We will use brute force to attack this router.

D. ROUTER R2

Router R2 will work like Router R1. We will use all the techniques and procedures that were used in Router R1. We will Bot and automatic Data Hiding Attack on Router R2. The user will first enter the user ID and password, and then the user will enter the port number. If a user steals a key using a keylogger, HIDS will check all incoming keys and match existing keys. If all the keys in step 1 and step 2 match the existing keys, it will provide access to the user. We will use eth-1 to connect different client PCs with Router R2.

E. USER ROUTING PROTOCOL (URP)

UPR is an interface that will act as an interface. The function of URP will that it will connect multiple routers and clients of routers with a cloud server. We will assign port number 5162 to the URP router. When clients of routers (R1 and R2) and routers want to connect to the cloud server, they will communicate via URP. We will use NIDS and Firewall with URP to protect the cloud server.

F. HOST BASED INTRUSION DETECTION SYSTEM (HIDS)

HIDS's job is to monitor incoming Host packets and detect malicious activities from packets. If an unauthorized person tries to access the cloud using invalid keys, HIDS will check the keys, then allow or disallow the user.

G. NETWORK BASED INTRUSION DETECTION SYSTEM (NIDS)

When the routers (R1 and R2) connect to the URP, NIDS will monitor packets across the network and check incoming activity on the URP and cloud server.

H. FIREWALL

The function of the firewall is that when the routers (R1 and R2) are connected to the URP and try to retrieve data from the cloud server, NIDS will monitor the packet and if the packets are malicious, so firewall will block it.

I. CLOUD SERVER

The cloud server will act as a data center where all the data will be stored. we will use port number 5745 for cloud server. We will not connect any router directly to the cloud server so that attacks on the cloud server are minimized or not. We will connect the cloud server to the URP via *serial 0/1*. We will DDoS attack on the cloud server because the cloud server is secure and powerful and can only be accessed using URP. There are two possibilities for DDOS to attack a cloud server. If a URP user attacks the cloud server and the other is if a user accesses the cloud server using URP. In this article we will attack the cloud server by URP user.

IV. EXPERMIMENTS

A. ATTACKS ON ROUTER R1

Whenever an invalid user tries to access the cloud server, invalid user always uses pattern matching techniques. The keys are estimated using pattern matching. This paper has designed a framework to protect the cloud server from pattern matching attacks so that the user can search or insert the keys for a limited time. After this limited time, that IP address will not be able to access the cloud server.

Router R1 has been attacked with pattern matching and HIDS has been used to protect the cloud server from pattern matching attacks. R1 consist of 16-users and each user provide a unique Login ID and Password. Suppose a user enters an incorrect user ID, password, or both, then the cloud server gives him a second chance to re-enter the keys. If the user enters the wrong key a second time, the cloud server gives him one last chance, but repeatedly inserting the wrong keys means that this is an invalid user who is trying to guesses the keys repeatedly. In this case, the Host-Based Intrusion Detection System detected the intrusion by the host and generated multiple alerts at a time, as shown in Fig 2.

```
nwa -dev -d/etc/files/nwa/Snwpy
Running in WN-mode

            ---=Initializing tool==--
Initializing output plugins!
Initializing Preprocessor!
Initializing database Files!
Initializing plug-ins!
Parsing Rules file "etc/files/nwa/snwpy"
PortCon  'FTP_PORT' defined  :  [20]
PortCon  'SHELLCODE_PORTS' defined  :  [0:79  81:65534]
PortCon  'ORACLE_PORTS' defined  :  [1521]
Packet Limits: 256

Loading Files            75%[===============     ] 63kB/s

nw@zpx-login:  admin
[admin]@zpx-password:  *****
root@zpx_DATABASE:  invalid operation
Try 'root --help' for more informations
nw@zpx-login:  nadeem_db
[nadeem_db]@zpx-password:  ******
root@zpx_DATABASE:  invalid operation
[help]-zpx-alert:  exit/continue
root@zpx-select  continue
nw@zpx-login:  ali_arshad72
[ali_arshad]@zpx-password:  *****
Disconnect $PATH_CLD_database
Disconnect $PATH_CLD_files
Disconnect $PATH_CLD_user
Disconnect $PATH_CLD_misc
```

FIGURE 2. Detection of intrusion using invalid keys.

When the right user forgot the keys and entered the wrong keys in the first attempt, a second chance was given. If the second time also entered the wrong keys, a last chance was given. A right user will consider the wrong user because of using repeatedly wrong keys. If the user forgets the keys, the keys can be recovered via two-step verification. If the user enters incorrect keys and then entered the correct keys. The user must verify the account in order to identify the correct user and incorrect user as shown in Fig 3 and prevent the cloud server from being misused.

Instead of using a graphical user interface to provide effective security to the cloud, various commands were developed and worked on it. Each command is given a unique functionality. *"ipdispall"* is the first command, whose job is to show all the devices which accessing the Router R1, as shown in Fig 4. The second command is *"ipconfigdet_ipaddress"* that is used inside the *"ipdisplall"* command to display the status of any PC. Fig 5 accessed the status of PC-3 by using the *"ipconfigdet192.168.15.3"* command.

Two-parent commands were created in Router R1. One is *"ipdispall"*, and the other is *"ipdataaccess"*. A command

```
nwa -dev -d/etc/files/nwa/Snwpy
Running in WN-mode

            ---=Initializing tool==--
Initializing output plugins!
Initializing Preprocessor!
Initializing database Files!
Initializing plug-ins!
Parsing Rules file "etc/files/nwa/snwpy"
PortCon  'FTP_PORT' defined  :  [20]
PortCon  'SHELLCODE_PORTS' defined  :  [0:79  81:65534]
PortCon  'ORACLE_PORTS' defined  :  [1521]
Packet Limits: 256

Loading Files            75%[===============     ] 63kB/s

nw@zpx-login:  db_studio_pro
[db_studio_pro]@zpx-password:  *****
root@zpx_DATABASE:  invalid operation
Try 'root --help' for more informations
nw@zpx-login:  SYSTEM
[SYSTEM]@zpx-password:  ******
[PORT]-zpx-:  3295
[Verification]-zpx-account:  system_db@gmail.com
root@zpx_DATABASE:  Account is verified Successfully..
[SYSTEM]@zpx-show:
```

FIGURE 3. Result of user identification.

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

Devices	Protocols	Status	DNS-Suffix
Dell 5745	192.168.1.1	Connected	Dlink
Xvds	192.168.1.2	Connected	Tenda
HP 4510	192.168.1.3	Connected	vlink_n3305
R4sh	192.168.1.4	Connected	Netgear C300
Workstation Z1	192.168.1.5	Connected	Linksys WR30
Thinkpad 24d	192.168.1.6	Connected	Dlink
Lenovo c5	192.168.1.7	Connected	DIR-X6060
Dell 452s	192.168.1.8	Connected	Dlink
Toshiba b4	192.168.1.9	Connected	Netgear Orbi
Samsung	192.168.1.10	Connected	DWR-921
Iphone 12	192.168.1.11	Connected	Tenda N301
Thinkpad X1 Carbon	192.168.1.12	Connected	PTCL-2054
Thinkpad 24d	192.168.1.13	Connected	AC1200
Lenovo c5	192.168.1.14	Connected	Dlink
LG g1	192.168.1.15	Connected	Linksys EA950
Vivo S1 Pro	192.168.1.16	Connected	Tenda Z500

FIGURE 4. Various connected devices with Router R1.

name *"ipconfigdet_ipaddress" is* a subcommand of *"ipdispall"*. The functionality of *"ipdispall"* is that it will display the IP address of each PC, which have already discussed. The second command is, *"ipdataaccess"*. With the help of this command, various data was viewed on the cloud servers of Router R1. Router R1 data can be accessed using file numbers instead of various commands.

Prevention From Pattern Matching Attacks: The best way to prevent cloud servers from attacking pattern matching is to give the user limited access to login keys. The cloud server should then be locked for a while, but when the key is inserted repeatedly, the IP address should be blocked for 24 to 48 hours. The advantage of blocking IP address is that pattern matching will not be possible with this IP address. Until unlocked it.

To show the better results of Router R1, a mathematical law was used to accurately represent the product and prove its accuracy as shown in Table 2. The user cannot enter the port number until use the valid user-ID and password.

The results of Router R1 are enforced in the Commutative Act where the *user-ID* is represented by "*A*" and the

```
nw@zpx-login:  SYSTEM
[SYSTEM]@zpx-password:  ******
[PORT]-zpx-:  3295
[SYSTEM]@zpx-show: ipconfigdet_192.168.15.3

root@zpx_DATABASE: Pinging 192.168.15.3 with 32 bytes of data:
PORT  STATE SERVICE
MAC Address: F8:2C:15:4J:73:12
Network Distannce: 1 hop

Please Wait...
root@zpx_DATABASE:192.168.15.3 is connected...

Ping Stistics for 192.168.15.3
Packets: Sent = 4, Recieved = 4, Lost = 0

Ethernet adapter Ethernet:
        Media Status.....................................: Connected
        Connection-specific DNS suffix ..................: V_link_n3005


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


Ethernet adapter Detail:
        IPV4 address.....................................: 192.168.15.3
        Port Number .....................................: 3295
        Link-local IPV6 address .........................: 2002:c0a8:0101::c
        Subnet Mask .....................................: 255.255.255.0
        Default Gateway .................................: 13.128.0.0
```

FIGURE 5. Status of IP address 192.168.15.3 of Router R1.

TABLE 2. Resultf of router R1 by using commutative law.

A *(User ID)*	B *(Pass)*	X (A*B)	Y (Port Accessibility)	C (Port Number)	X^C	C^X
F	F	Not Accessible	✗	✗	Not Accessible	Not Accessible
F	T	Not Accessible	✗	✗	Not Accessible	Not Accessible
T	F	Not Accessible	✗	✗	Not Accessible	Not Accessible
T	T	Accessible	✓	T	Accessible	Accessible
T	T	Accessible	✓	F	Not Accessible	Not Accessible

password is represented by "*B*". "*X*" is the result of accessing the cloud. Unless "*A*" and "*B*" are correct, access to the port will not be possible. Port accessibility is represented by "*Y*". When the user enters the correct *user-ID* and *password*, the port is then accessed. Port number is represented by "*C*". If "*X*" = *True* and "*C*" = *False*. So be it *X^C* or *C^X*, in both case, cloud access is not possible, which is shown in Table-2. If "*X*" = *True* and "*C*" = *True*, So be it *X^C* or *C^X*, in both case, cloud access is possible.

B. ATTACKS ON ROUTER R2

Two attacks were carried on router R1. One attack was made while accessing the router. When repeatedly trying to access the router using the wrong keys, which is shown in Fig 1. While the second attacked was done by brute force. If the intruder gets the user ID of any user, the attacker can search for the password using brute force. We used two-step verification for Router R2.

Whenever an attacker attacks a cloud server, the first attempt of an attacker is Pattern Matching. With the help of which attacker enters every password he deems possible, but when there will be a signature matching prevention technique in the cloud which has already been discussed in this article, the attacker will use another technique that is Brute Force can be used in two ways. The first use is to create a dictionary and attack the cloud server using this dictionary and the second use is to design an algorithm and attack the cloud with this algorithm. The dictionary attacked has been done in this

```
admhy 1883401
admhz 1883402
admh0 1883403
admh1 1883404
admh2 1883405
admh3 1883406
admh4 1883407
admh5 1883408
admh6 1883409
admh7 1883410
admh8 1883411
admh9 1883412
admia 1883413
admib 1883414
admic 1883415
admid 1883416
admie 1883417
admif 1883418
admig 1883419
admih 1883420
admii 1883421
admij 1883422
admik 1883423
admil 1883424
admim 1883425
password is admin. found in 1883426 guesses.
```

FIGURE 6. Result of Brute Force Attack.

paper in which different passwords have been searched and it has been concluded that the longer the password length, the harder it will be to search for passwords. In Figure 6, the password = "admin" is found after 2 hours and 43 minutes. The Index number of this password has been found is "1883426". Passwords are less likely to be attacked if they contain special symbols and uppercase letters.

Prevention Form Brute Force Attack: Cloud servers can be protected from Brute attacks in three ways. The first solution is to use two-step verification techniques. If a user obtains a cloud password using brute force, the cloud server will require two-step verification from the user. Then grant access to the cloud server. The second solution is that when the user accesses the cloud server, the user must verify OTP before accessing. The third solution is that the password length should be greater than 8, including at least two capital letters and two special symbols. Special symbols are safe and Brute Force attack do not work on the special symbols and there are very rarely chances of brute force attacks on special symbols. The longer and more secure the password, the harder the attack will be.

After testing Router R2, all the results of Router R2 were applied to the mathematical property called *"identity property"* and two numbers (0 and 1) were used to indicate the accuracy and error of the results. 0 indicates incorrect results while 1 indicates correct results. According to *"identity property"*, if multiply the correct number by 1, the result will be correct. Conversely, if multiply the correct number by 0, the result will be incorrect. Apply this property to Router R2 results where User-ID and password are equal to X and port number is equal to Y as shown in Table 3. Such as *User-Id* + *Password* = *X* and *port number* = *Y*.

Suppose Y = 0, when X is multiplied by Y, the output will be zero, which means that Router R2 will not be accessible. Similarly, if Y = 1, when X multiplied by Y, the output will be 1, which means that Router R2 will be accessible due to the correct user-ID, password, and correct port number.

C. USER ROUTING PROTOCOL (URP)

The URP used an interface called Business Layer to connect the Router R1 and the router R2 to the cloud server. The URP

TABLE 3. Resultf of router R2 by using identity property.

Step-1 Verification			Step-2 Verification		Results	
User-ID	Password	Result	Port Accessibility	Port Number	Identity Property (X*Y)	Router R2 Accessibility
A	B	X= A*B	C	Y	Z	✖
0	0	0	✖	✖	✖	✖
0	1	0	✖	✖	✖	✖
1	0	0	✖	✖	✖	✖
1	1	1	✓	0	0	✖
1	1	1	✓	1	1	✓

has two users and is granted full access to Router R1 and Router R2. The URP router uses the command *"ipshortport"* that displays the sub-ports connected to the router, as shown in Fig 7.

```
[SYSTEM]@zpx-show:  ipshortport
root@zpx_DATABASE:  Ports Searching

ROUTER    NID             BID             SM              RATE        STATUS
-------------------------------------------------------------------------------

R1        13.128.0.0      13.191.0.0      255.192.0.0     4Mbit/s     Acitve
R2        13.192.0.0      13.255.0.0      255.192.0.0     7Mbit/s     Acitve
```

FIGURE 7. URP connected Ports.

D. ATTACKS ON CLOUD SERVER

In this paper, the cloud server acted as the data center. Cloud server can only be accessed through URP router, no other router can access cloud server directly. An internal attack on the cloud server may be possible through the cloud server user. DDoS attacks were carried out inside the cloud server in which the attackers sent various bots to the cloud server.

When an attacker wants to access or distort cloud server data, the attacker will send spam in the form of a bot, as shown in Fig 8. This bot will have an injection that will hide all data from the bot cloud server as soon as this bot offer is accepted. If the bot offer is rejected, the cloud server will return to normal.

When the user accepts the attacker's offer, the bot of cloud deletes and corrupts all the data on the cloud server without any information. If the user does not agree with DDoS's offer, the figure Fig 9 will appear on the screen after a while. In this Bot, the attacker uses a new phishing technique in the message. The attacker detected 40 infected files from cloud servers. These files are not in the cloud server but the attacker uses this message to deceive us.

There are two options in the bot of Fig 9. One is to delete infectious files using the "*Remove*" command and the other is to keep infectious files using the "Continue" command. If type the command "Remove", the cloud server will be attacked by a bot and all the data of a cloud server will be deleted and corrupted.

If type the "*Continue*" command, then the bot will disappear from the cloud server screen and after a while it will come with a new name, shown in Fig 10. The attacker will remain to send these types of zombies again and again until accept it. Here are two other DDoS zombies are shown in Fig 9 and Fig 10.

```
        C O N G R A T U L A T I O N

You've been chosen to recieve a
        FREE Gateway Desktop Computer!

      >> Intel Pentium 4 Processor 2.66 GHZ
      >> 8GB DDR4 SDRAM, 2TB Hardisk
      >> 19-inch Color LED with free Cable

Enter "Accept" to Claim your FREE Desktop Computer!
Enter "Reject" for EXIT

         Accept                    Reject

        _________                 ___________
SYSTEM:>
```

FIGURE 8. First DDoS Attack on Cloud Server.

```
              W  A  R  N  I  N  G
        4 0  i n f e c t i o n s  f o u n d !!!!!!!!!!!

Last scan detected malicious programs(4), ciruses(6),adware(18),
spyware(5),tracking cookies(7).

 These harmfull programs can cause:
 These garmfull programs can cause:

   (x) System crash

   (x) Permanent Data Loss

   (x) System startup failures

   (x) System Slowdown

   (x) Internet connection Loss

   (x) Infecting other computer on your network

Enter "Remove" for THREAT REMOVE
Enter "Continue" CONTINUE UNPROTECTED

        Remove                    Continue

      ___________               ______________
SYSTEM:>
```

FIGURE 9. Second DDoS Attack on Cloud Server.

If do not accept DDoS bot request, cloud server will not be attacked and as soon as accept the request, DDoS will attack the cloud server and all data will be deleted from the cloud server, shown in Fig 11.

Prevention Form DDoS Attack: The cloud can be protected from DDoS in two ways. The first method is to permanently block the IP address if the attacker is sending DDOS using a static IP address. Alternatively, if the attacker is attacking DDoS via a dynamic IP address, the best solution is to use Cloudflare for the cloud server. But Cloudflare should act as an interface. Whenever different addresses try to access the cloud server, only the IP addresses that the cloud server allows access to the cloud server. Cloudflare should block all other invalid addresses as shown in Fig-12, which greatly reduces the chances of DDoS attacks on the cloud server.

E. COMPARATIVE ANALYSIS

Various researchers have researched and developed many algorithms to keep the cloud server safe and protect the data from suspicious attack. In 2018, researchers reviewed different DDoS attacks using different data mining algorithms [11] and worked on the Fuzzy c-means algorithm. The authors found a DDoS attack rate that was 98.7% and DDoS attack detection time was 0.15 seconds. In 2019, Researchers suggested two ways to detect DDoS attacks [12]. One is the

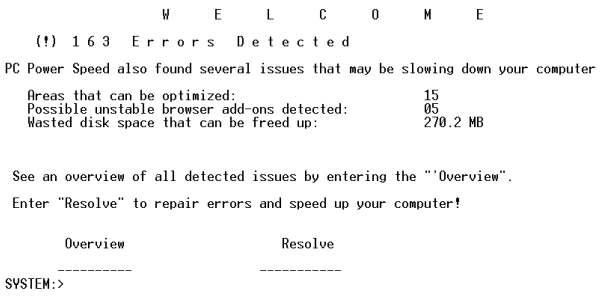

FIGURE 10. Third DDoS attack on the cloud server.

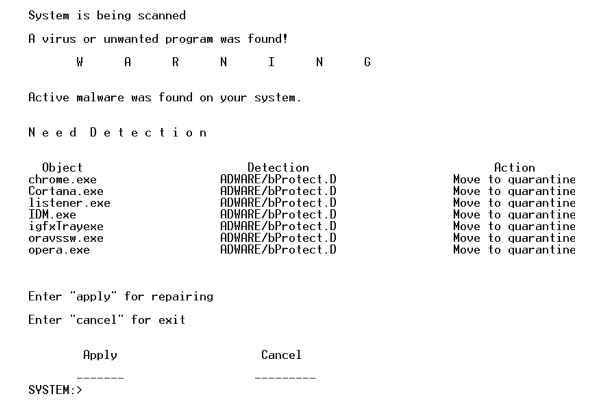

FIGURE 11. Fourth DDoS attack on the cloud server.

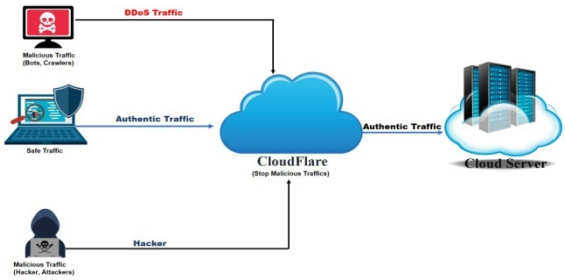

FIGURE 12. DDoS prevention by Cloudflare.

degree of attack and the other is the use of ML algorithm and discussed that the accuracy of ML (DDAML) is better than KNN, SVM and CIC-SVM algorithms. In 2020, Researchers have worked on cloud security challenges [1] and discussed that if the cloud is protected from the surface, then very rarely chances of malware attacks on the cloud servers, after that discussed several attacks, threats, and models for the cloud server. In 2020, researchers proposed an automated host-based framework and linked the user and kernel spaces by using some machine learning techniques and detected Intrusion from smart devices. In 2021, researchers reviewed various papers on DDoS attacks [8] and discussed the various causes of DOS attacks. After review, worked on Random Forest and CatBoost algorithms and discussed all possible types of DDoS attacks on each layer of the OSI model and showed that the accuracy of Random Forest and CatBoost algorithms is 99.99% that is very high.

Many researchers have worked on different algorithm and obtained different results from these algorithms but none of the researchers have experimentally proved the accuracy of the algorithm and have not discussed which technique can prevent the cloud from various attacks. If an attacker attacks a cloud server, how can the cloud be prevented from attack.

This article developed an effective framework for providing security to the cloud server and experimentally demonstrated that if a set of principles and mechanisms are applied to each cloud server device, the cloud is protected from both internal and external sides. After that discussed all possible types of attacks that intruders typically use to attack on a cloud server and disrupt the functionality of cloud server and it was concluded that if a secure mechanism is implemented on the cloud server, then the cloud server can be protected from various attacks. If cloud servers and all devices of cloud server are secure, then there is less chances of a cloud server attacks. A cloud can be secure if its algorithm is secure

V. CONCLUSION

After developing and testing the software concluded that an intrusion detection system is an excellent technique for catching intervention from the cloud. Cloud can be protected from intrusion attacks if a secure algorithm for cloud computing is developed Clouds can only be secured when a secure architecture design for it. When an attacker tries to steal keys using spyware, the attacker can immediately access the cloud. The cloud can be saved if an alert and signature system is used in the cloud. Strict warnings can be issued if the attacker repeatedly enters the wrong keys. Cloud servers should use different authentication methods to provide better security, such as encryption, two-step authentication techniques, signatures, and so on.

This article develops an effective tool and then builds an architecture that uses HIDS, SIDS and NIDS to protect the various routers and cloud servers. The cloud server was then attacked in three different scenarios. In the first scenario, attacked Router R1. In the second scenario, attacked Router R2, and in the third scenario, attacked on the cloud server. Different tables were set for each scenario after the attack. and implemented the different laws into tables to check the table result accuracy. In conclusion, a cloud intrusion can be prevented if a better way is used to detect cloud intrusion as well as protect it from attacks.

In future, a secure algorithm will be developed for the cloud and will check the effect of various components of the system (RAM, CPU, and cache) in time of Intrusion Detection System (IDS) execution and will also compare multiple tools such as Snort, Suricata, OSSEC with this tool and develop a better algorithms and techniques for this tool and secure the cloud.

REFERENCES

[1] N. R. Tadapaneni and S. S. H. Hussaini, "Cloud computing security challenges," *SSRN Electron. J.*, vol. 11, no. 7, pp. 1–6, 2020.
[2] J. Snehi, "Diverse methods for signature based intrusion detection schemes adopted," *Int. J. Recent Technol. Eng.*, vol. 9, no. 2, pp. 44–49, 2020.

[3] A. A. Aryachandra, Y. F. Arif, and S. N. Anggis, "Intrusion detection system (IDS) server placement analysis in cloud computing," in *Proc. 4th Int. Conf. Inf. Commun. Technol. (ICoICT)*, May 2016, pp. 1–5.
[4] N. R. Tadapaneni, "Cloud computing: Opportunities and challenges," *SSRN Electron. J.*, vol. 6, no. 9, pp. 122–143, 2018.
[5] R. Gassais, N. Ezzati-Jivan, J. M. Fernandez, D. Aloise, and M. R. Dagenais, "Multi-level host-based intrusion detection system for Internet of Things," *J. Cloud Comput.*, vol. 9, no. 1, pp. 1–16, Dec. 2020.
[6] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, Aug. 2014.
[7] M. Mazini, B. Shirazi, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 31, no. 4, pp. 541–553, Oct. 2019.
[8] V. Vishal and K. Vasudha, "DoS/DDoS attack detection using machine learning: A review," in *Proc. Int. Conf. Innov. Comput. Commun. (ICICC)*, 2021, pp. 1–7.
[9] N. Jyoti and S. Behal, "A meta-evaluation of machine learning techniques for detection of DDoS attacks," in *Proc. 8th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, 2021, pp. 522–526.
[10] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020.
[11] S. Sumathi and N. Karthikeyan, "Search for effective data mining algorithm for network based intrusion detection (NIDS)-DDoS attacks," in *Proc. Int. Conf. Intell. Comput. Commun. Smart World (ICSW)*, Erode, India, Dec. 2018, pp. 41–45.
[12] S. Dong and M. Sarem, "DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2020.
[13] X. Li, W. Chen, Q. Zhang, and L. Wu, "Building auto-encoder intrusion detection system based on random forest feature selection," *Comput. Secur.*, vol. 95, Aug. 2020, Art. no. 101851.
[14] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101752.
[15] R. Abdulhammed, H. Musafer, A. Alessa, M. Faezipour, and A. Abuzneid, "Features dimensionality reduction approaches for machine learning based network intrusion detection," *Electronics*, vol. 8, no. 3, p. 322, Mar. 2019.
[16] N. N. Tuan, P. H. Hung, N. D. Nghia, N. Van Tho, T. V. Phan, and N. H. Thanh, "A robust TCP-SYN flood mitigation scheme using machine learning based on SDN," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2019, pp. 363–368.
[17] N. Bakhareva, A. Shukhman, A. Matveev, P. Polezhaev, Y. Ushakov, and L. Legashev, "Attack detection in enterprise networks by machine learning methods," in *Proc. Int. Russian Automat. Conf. (RusAutoCon)*, Sep. 2019, pp. 1–6.
[18] M. Poongodi, M. Hamdi, A. Sharma, M. Ma, and P. K. Singh, "DDoS detection mechanism using trust-based evaluation system in VANET," *IEEE Access*, vol. 7, pp. 183532–183544, 2019.
[19] Ç. Ateş, S. Özdel, and E. Anarım, "Clustering based DDoS attack detection using the relationship between packet headers," in *Proc. Innov. Intell. Syst. Appl. Conf. (ASYU)*, Oct. 2019, pp. 1–6.
[20] K. Wehbi, L. Hong, T. Al-Salah, and A. A. Bhutta, "A survey on machine learning based detection on DDoS attacks for IoT systems," in *Proc. SoutheastCon*, Huntsville, AL, USA, Apr. 2019, pp. 1–6.
[21] R. U. Khan, X. Zhang, M. Alazab, and R. Kumar, "An improved convolutional neural network model for intrusion detection in networks," in *Proc. Cybersecurity Cyberforensics Conf. (CCC)*, May 2019, pp. 74–77.
[22] F. S. D. L. Filho, F. A. F. Silveira, A. de Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, "Smart detection: An online approach for DoS/DDoS attack detection using machine learning," *Secur. Commun. Netw.*, vol. 2019, pp. 1–15, Oct. 2019.
[23] Z. He, T. Zhang, and R. B. Lee, "Machine learning based DDoS attack detection from source side in cloud," in *Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, Jun. 2017, pp. 114–120.
[24] J. Zhang, "Detection of network protection security vulnerability intrusion based on data mining," *Int. J. Netw. Secur.*, vol. 21, no. 6, pp. 979–984, 2019.
[25] G. Kaur and P. Gupta, "Hybrid approach for detecting DDoS attacks in software defined networks," in *Proc. 12nd Int. Conf. Contemp. Comput. (IC)*, Noida, India, Aug. 2019, pp. 1–6.
[26] P. Narwal, D. Kumar, and S. N. Singh, "A hidden Markov model combined with Markov games for intrusion detection in cloud," *J. Cases Inf. Technol.*, vol. 21, no. 4, pp. 14–26, Oct. 2019.
[27] A. Yang, Y. Zhuansun, C. Liu, J. Li, and C. Zhang, "Design of intrusion detection system for Internet of Things based on improved BP neural network," *IEEE Access*, vol. 7, pp. 106043–106052, 2019.
[28] B. A. Tama, M. Comuzzi, and K. Rhee, "TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system," *IEEE Access*, vol. 7, pp. 94497–94507, 2019.
[29] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Dec. 2019.
[30] P. K. Singh, S. K. Jha, S. K. Nandi, and S. Nandi, "ML-based approach to detect DDoS attack in V2I communication under SDN architecture," in *Proc. IEEE Region Conf. (TENCON)*, Oct. 2018, pp. 144–149.
[31] A. Khraisat, I. Gondal, and P. Vamplew, "An anomaly intrusion detection system using C5 decision tree classifier," in *Trends and Applications in Knowledge Discovery and Data Mining*. Cham, Switzerland: Springer, 2018, pp. 149–155.
[32] J. Lyngdoh, M. I. Hussain, S. Majaw, and H. K. Kalita, "An intrusion detection method using artificial immune system approach," in *Proc. Int. Conf. Adv. Informat. Comput. Res.*, 2018, pp. 379–387.
[33] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, 2018, pp. 108–116.
[34] S. Ustebay, Z. Turgut, and M. A. Aydin, "Intrusion detection system with recursive feature elimination by using random forest and deep learning classifier," in *Proc. Int. Congr. Big Data, Deep Learn. Fighting Cyber Terrorism (IBIGDELFT)*, Dec. 2018, pp. 71–76.
[35] S. Wankhede and D. Kshirsagar, "DoS attack detection using machine learning and neural network," in *Proc. 4th Int. Conf. Comput. Commun. Control Automat. (ICCUBEA)*, Aug. 2018, pp. 1–5.
[36] B. J. Radford, B. D. Richardson, and S. E. Davis, "Sequence aggregation rules for anomaly detection in computer network traffic," in *Proc. Amer. Stat. Assoc. Symp. Data Sci. Statist.*, 2018, pp. 1–13.
[37] K. S. Hoon, K. C. Yeo, S. Azam, B. Shunmugam, and F. De Boer, "Critical review of machine learning approaches to apply big data analytics in DDoS forensics," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2018, pp. 2–6.
[38] S. Soheily-Khah, P. Marteau, and N. Béchet, "Intrusion detection in network systems through hybrid supervised and unsupervised machine learning process: A case study on the ISCX dataset," in *Proc. 1st Int. Conf. Data Intell. Secur. (ICDIS)*, Apr. 2018, pp. 219–226.
[39] F. Farahnakian and J. Heikkonen, "Anomaly-based intrusion detection using deep neural networks," *Int. J. Digit. Content Technol. Appl.*, vol. 12, pp. 70–118, Oct. 2018.
[40] T. Qian, Y. Wang, M. Zhang, and J. Liu, "Intrusion detection method based on deep neural network," *Huazhong Keji Daxue Xuebao*, vol. 46, no. 1, pp. 6–10, 2018.
[41] R. Priyadharshini and E. J. Leavline, "Cuckoo optimisation based intrusion detection system for cloud computing," *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, no. 11, pp. 42–49, Nov. 2018.
[42] A. Jayaswal and R. Nahar, "Detecting network intrusion through a deep learning approach," *Int. J. Comput. Appl.*, vol. 180, no. 14, pp. 15–19, Jan. 2018.
[43] H. Ji, Y. Wang, H. Qin, Y. Wang, and H. Li, "Comparative performance evaluation of intrusion detection methods for in-vehicle networks," *IEEE Access*, vol. 6, pp. 37523–37532, 2018.
[44] Q. Xiong, Y. Xu, B.-F. Zhang, and F. Wang, "Overview of the evasion resilience testing technology for network based intrusion protecting devices," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, Jan. 2017, pp. 146–152.
[45] H. Shapoorifard and P. Shamsinejad, "Intrusion detection using a novel hybrid method incorporating an improved KNN," *Int. J. Comput. Appl.*, vol. 173, no. 1, pp. 5–9, Sep. 2017.
[46] M. A. Jabbar, R. Aluvalu, and S. S. Reddy, "RFAODE: A novel ensemble intrusion detection system," *Proc. Comput. Sci.*, vol. 115, pp. 226–234, Jan. 2017.
[47] C. She, W. Wen, Z. Lin, and K. Zheng, "Application-layer DDoS detection based on a one-class support vector machine," *Int. J. Netw. Secur. Appl.*, vol. 9, pp. 13–24, Jan. 2017.
[48] S. Daneshgadeh, N. Baykal, and S. Ertekin, "DDoS attack modeling and detection using SMO," in *Proc. 16th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2017, pp. 432–436.

[49] S.-Y. Ji, B.-K. Jeong, S. Choi, and D. H. Jeong, "A multi-level intrusion detection method for abnormal network behaviors," *J. Netw. Comput. Appl.*, vol. 62, pp. 9–17, Feb. 2016.
[50] V. Singh and S. Puthran, "Intrusion detection system using data mining a review," in *Proc. Int. Conf. Global Trends Signal Process., Inf. Comput. Commun. (ICGTSPICC)*, Jalgaon, India, Dec. 2016, pp. 587–592.
[51] D. P. Gaikwad and R. C. Thool, "Intrusion detection system using bagging ensemble method of machine learning," in *Proc. Int. Conf. Comput. Commun. Control Automat.*, Feb. 2015, pp. 291–295.
[52] O. Can and O. K. Sahingoz, "A survey of intrusion detection systems in wireless sensor networks," in *Proc. 6th Int. Conf. Modeling, Simulation, Appl. Optim. (ICMSAO)*, May 2015, pp. 1–6.
[53] S. Elhag, A. Fernández, A. Bawakid, S. Alshomrani, and F. Herrera, "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems," *Expert Syst. Appl.*, vol. 42, no. 1, pp. 193–202, 2015.
[54] P. S. Kenkre, A. Pai, and L. Colaco, "Real time intrusion detection and prevention system," in *Proc. 3rd Int. Conf. Frontiers Intell. Comput., Theory Appl. (FICTA)*. Cham, Switzerland: Springer, 2015, pp. 405–411.
[55] W.-C. Lin, S.-W. Ke, and C.-F. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," *Knowl.-Based Syst.*, vol. 78, pp. 13–21, Apr. 2015.

MUHAMMAD NADEEM received the B.S. degree in computer science from Preston University and the M.Sc. degree in computer science from Abasyn University, Islamabad, Pakistan. His research interests include cloud security and intrusion detection systems.

ALI ARSHAD received the B.S. degree in computer science from Iqra University, Pakistan, in 2008, the M.S. degree in software engineering from International Islamic University, Pakistan, in 2012, and the Ph.D. degree in computer science and technology from Xidian University, China. He is currently an Assistant Professor with the Institute of Space and Technology, Islamabad, Pakistan. He has published high-quality articles in refereed international SCI-IF journals. His research interests include machine learning, semi-supervised learning, and fuzzy c mean clustering.

SAMAN RIAZ received the M.Sc. and M.Phil. degrees in applied mathematics from Quaid-e-Azam, Pakistan, in 2006 and 2008, respectively, and the Ph.D. degree in computer science and technology from Xidian University, China. She is currently an Assistant Professor with the National University of Technology, Islamabad, Pakistan. Her research interests include deep learning and probability.

SHAHAB S. BAND (Senior Member, IEEE) received the M.Sc. degree in artificial intelligence and the Ph.D. degree in computer science from the University of Malaya, Kuala Lumpur, Malaysia. He is currently an Adjunct Professor with Ton Duc Thang University, Vietnam. He is also an Adjunct Faculty with Iran Science and Technology University, Iran. He is also an Academic Faculty with IAUC, Iran. He is also a Faculty Member with the University of Malaya, Malaysia. He is also a Postdoctoral Research Fellow. He has published more than 200 articles, in refereed international SCI-IF journals (100), international conference proceedings (25), books (ten) with more than 7000 citations in Google Scholar (with H-index of 29), and ResearchGate RG Score of 47. He has worked on various funded projects. His major research interests include computational intelligence and data mining in multidisciplinary fields. His articles are ranked in the highly cited articles and most downloaded articles from the top 10 % (2013 till now) in computer science according to the WoS. He is on the editorial board of journals and has served as a guest editor for journals.

AMIR MOSAVI received the Ph.D. degree in applied informatics. He is currently an Alexander von Humboldt Research Fellow for big data, the IoT, and machine learning. He is a Senior Research Fellow at Oxford Brookes University. He is a Data Scientist for climate change, sustainability, and hazard prediction. He was a recipient of the Green-Talent Award, the UNESCO Young Scientist Award, the ERCIM Alain Bensoussan Fellowship Award, the Campus France Fellowship Award, the Campus Hungary Fellowship Award, and the Endeavour-Australia Leadership.