Received: December 12, 2019

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A New Cybersecurity Approach for Protecting Cloud Services against DDoS Attacks

Hosam F. El-Sofany[1, 2]*

[1]*King Khalid University, Abha, Kingdom of Saudi Arabia*
[2]*Cairo Higher Institute for Engineering, Computer Science and Management, Cairo, Egypt*
* Corresponding author's Email: helsofany@kku.edu.sa

Abstract: Cybersecurity of cloud services is extremely important, especially when developing web services and cloud apps. Cloud computing depends on internet connections; therefore, the security of its services is constantly under attack. Distributed Denial of Service (DDoS) attacks are a malicious attempt to damage the normal traffic of the targeted cloud by flooding it with internet traffic. As a result, this causes a serious problem for cloud computing security. The objectives of this paper are, to introduce a new cybersecurity approach for protecting cloud services against all types of DDoS attacks, to evaluate the performance and effectiveness of the proposed algorithm, and to use the contribution of correlation coefficient analysis for validating the effectiveness of the proposed approach by identifying the relationship between malicious and legitimate traffic. The researcher evaluated the performance of the proposed approach in terms of accuracy, sensitivity, and specificity. The feedback of the experiments was highly promising for protecting cloud services against DDoS Attacks. The experiments showed encouraging results for preventing DDoS attacks, with an average performance of 95.41%, an average accuracy of 96.53%, an average sensitivity of 92.31%, and an average specificity of 97.39%.

Keywords: Cloud computing security, Cybersecurity, Cybercrime, Correlation analysis, Distributed denial of service attacks.

1. Introduction

Cloud computing is a successful internet-based architecture of service-oriented computing. It has led to the development of usage and management ways of computing infrastructure. It is a new paradigm for hosting resources and providing web services to consumers. In addition to the convenient access to a centralized shared pool of computing resources, cloud computing is deployed with efficiency using minimal management overhead. The cloud computing providers use internet communications as the main medium for delivering their IT resources to the organizations or individuals on a pay-as-you-use system [1]. Cloud computing has several definitions, but the main definition was introduced by the National Institute of Standards and Technology (NIST) [2]. According to this definition, cloud computing mode consists of three main service layers called SaaS, PaaS, and IaaS (i.e., software as a service, platform as a service, and infrastructure as a service). The cloud architecture consists of five essential components including clients, applications, platforms, infrastructure, and servers. The cloud model promotes availability and has integrated and essential characteristics such as availability, reliability, high elasticity, accessibility, high performance, and manageability. The cloud computing models are employed using four different deployment models: *private cloud*, in which cloud infrastructure is provided for private use in an organization; *community cloud*, in which cloud infrastructure is prepared for specific groups working in an organization; *public cloud*, where the cloud infrastructure is provided for open usage by the general public; and *hybrid cloud*, which consists of two or more previous clouds [3, 4].

Cloud security is highly important when we plan to develop cloud systems and services. The concerns

of cloud security are increasing because the customer's sensitive information is stored in a cloud provider server [5]. Therefore, cloud security researchers address these concerns by identifying some important objectives such as *availability* (the user can use the services from any location and at any time), *authentication* (users' identity should be assured), *accountability* (all users participate easily in a data transfer between the systems, and cloud services protects them from denial of service attacks), *confidentiality* (cloud servers should secure users' data, and no unauthorized individual can access the database), and integrity (the cloud model ensures that the data is not changed during storage, processing, and transport over the cloud).

The mentioned security goals need the innovation and implementation of novel security approaches and methodologies. A security mechanism is defined as "a process of detecting and preventing security attacks". Security service, on the other hand, is defined as "a processing service aimed to enhance the security of information transfer and help in countering security attacks" [6]. Whereas cloud systems use and share a large set of data, therefore the main motivations of attackers are to destroy these data and steal sensitive and valuable information. There are many cloud computing security attacks, but denial of service (DoS) attack is considered a dangerous attack targeting cloud security [7]. In DoS, the attacker overloads the target machine with numerous web requests that prevent the server from responding to any requests, and, hence, the network resources will be unavailable for their legitimate users. On the other hand, in DDoS attacks, attackers use serious machines called zombies to launch DoS attacks on the target machine, which infects the service and leads to delay or even total decline. Recently, DDoS attacks increased, targeting cloud systems, and hence suitable intrusion detection apps have to be released and published [8].

The cloud computing model needs new and innovative solutions to secure cloud provider infrastructure and users' resources such as data, information, applications, and services. Therefore, cloud security research is a new area of motivation for researchers. In this study, the researcher has focused on the DDoS attacks as an important issue that faces the security of cloud computing infrastructure.

In this research paper, the researcher introduces a new cybersecurity approach for detecting and preventing cloud services and systems against all types of DDoS attacks, instead of focusing on detecting one type of DDoS attack as most previous work. The main advantage of our proposed approach is starting with handling the client IP requests, detect them through three DDoS detectors, and prevent the input IP requests against volume-based, protocol-based, and application layer-based DDoS attacks. The author proposes an algorithm for securing cloud services from DDoS attacks. The performance measure and effectiveness of the proposed algorithm were evaluated in terms of accuracy, sensitivity, and specificity. The author used correlation coefficient analysis to validate the effectiveness of the proposed approach and to identify the relationship between malicious and legitimate traffic, as another contribution of this paper.

The rest of this paper is organized as follows. In section 3, the researcher introduces related work. Section three, introduces definitions, classification, and types of cybercrime on cloud services. Section four presents the importance of cybersecurity for ICT systems. Section five presents the DoS and DDoS cybersecurity attacks. In section six, the researcher introduces the proposed cybersecurity approach and presents the performance measure of the proposed algorithm. Section seven introduces the evaluation of the experimental results and presents the use of correlation coefficient analysis to validate the effectiveness of the proposed approach. The paper finally concluded in section eight.

2. Related work

R. Deshmukh et al. presented a study on DDoS attacks and their types with various countermeasures to mitigate the DDoS attacks using a survey. The presented survey covered DDoS detection and tolerance techniques, as well as providing some points to be considered while selecting DDoS defense solutions [9]. Another research report presented the famous top nine cloud computing threats in 2013, with descriptions and analysis of these threats. This report helped cloud users and providers to make informed decisions about risk mitigation within a cloud computing strategy [10]. R. Sarhadi et al. presented a cloud defender and self-learner system known as cloud service queuing defender (CSQD). This system is used to detect and prevent XML vulnerabilities in web services [11]. Moreover, a research study concluded that about 15% to 20% of the whole detected network attacks are classified as DoS attacks [12]. S. Padmanabhuni et al. proposed preventing service-oriented denial of service model called XDoS, to prevent denial of service attacks for XML. The proposed model works on content introspection to

detect any possible XDoS attacks [13]. A. Chonka et al. introduced a protector model based on a neural network to detect and filter DoS attacks. The researchers also presented a solution to determine the origin of the attack based on trace backing. The authors have used a Patricia Trie representation for comparing and evaluating the schemas and the request messages in an efficient way [14].

Recently, A. Bonguet et al. introduced a survey on DoS and DDoS attacks facing a cloud computing infrastructure. The research study allowed for showing most of the available countermeasures for XML and HTTP DoS attacks. The researchers evaluated the DoS and DDoS defenses, with appropriated metrics and experimental model [15]. M. Masdari et al. presented research on the effect of DoS attacks against virtual machines (VMs) and hypervisors connections. The authors introduced a network defense paradigm against DoS attacks [16]. O. Osanaiye et al. introduced a comprehensive survey for DDoS attacks targeting cloud servers. The researchers categorized the attacks into two levels and suggested an approach for detecting these attacks [17]. H. El-Sofany et al. presented a research study for DoS and DDoS attacks. They presented an experimental study showing the impact of DDoS attacks on cloud applications. The results of this research study figured out the need for a good mechanism to prevent DDoS attacks facing cloud applications in higher education organizations [18]. C. Amita et al. presented a study on the recent findings for the detection and prevention of DDoS attacks in SIP (Session Initiation Protocol) based Voice over IP (VoIP) networks. The authors also illustrated key issues that should be taken into consideration by the cybersecurity developer while designing attack detection systems against DDoS [31]. K. Naveen et al. proposed a new technique for the isolation of malicious nodes. In this research, the threshold-based technique was used for the detection of malicious nodes from the network. This approach used two parameters for the malicious node detection which are data rate and delay [32].

In this paper, the proposed approach provides a new cybersecurity approach for protecting cloud services against all DDoS attacks such as volume-based, protocol-based, and application layer-based DDoS attacks. The proposed approach considered as a more general model comparing with other approaches mentioned above such as the cloud defender system presented in [11-14], which focuses on the application-layer attacks to detect and prevent HTTP or XML-based DDoS attacks, as well as the system presented in [31, 32] which focuses on the detection and prevention of DDoS attacks in SIP-based Voice over IP networks.

3. Cybercrime on cloud computing

The term *cybercrime* is used to describe an illegal activity or set of activities in which computers or wireless computing devices (*e.g.*, mobiles, tablets, PDAs, etc.) are used as a tool for cybercrimes. It is often done by unethical people (called *cybercriminals*) for greed, revenge, theft, or adventure.

3.1 Classification of cybercrimes

The cloud applications, data, and services hosted in cloud computing servers could come under attack through *cybercriminals* [19]. The cybercriminal is categorized into an *internal* or *external* criminal by the organizations facing cyberattack. The organization infected by cyberattacks not only loses its financial situation but also loses its reputation. Cyberattacks on cloud systems are classified into structured and unstructured attacks based on the level of experience and power of the attackers.

- *Internal attack*: this attack infects the cloud systems by insider threats (*i.e.*, employees of cloud providers having authorized system access, and users misusing the cloud resources). It is easy for a person within the organization (insider) to do cyberattacks since he is well aware of the organization's policies, network access, and cloud system security. Therefore, it is easy for an insider to steal information, change sensitive data, deactivate some process, and deny cloud services. This attack might be detected and prevented by good planning and setting up internal Intrusion Detection Systems (IDS).
- *External attack*: this attack comes from cybercriminals who are not part of the cloud environments (*i.e.*, it infects the cloud systems by attackers from outside of the organization). The cloud system administrator is responsible for detecting and preventing these external attacks by using firewalls programs or IDS.
- *Structured attack*: this attack is achieved by highly experienced attackers with clear policy and motivations in their minds. They could be able to access the cloud system security without being noticed by the IDS systems. These attackers have sophisticated tools and technologies to hide. This level of attack is usually achieved by professional criminals of rival countries, to damage specific

persons or countries, or rival companies, and so on.

- *Unstructured attack*: this attack is developed by beginner attackers who do not have any specified motivations to perform the cyberattacks. They generally try to test their tools of attack over the internet to infect random companies, organizations, or private websites.

Recently, cybercrimes offer on-demand cloud and internet services by some cybercriminals. In this case, the customer (person, company, organization, or country) contacts with cybercriminals for hacking their competitor web portal to gain required sensitive data, or perform a denial of service attack. Based on customer requirements, hackers write malware or virus programs to hack the competitor network

3.2 Types of cybercrimes

There are numerous types of cybercrimes as follows [20]:

- *Cyberterrorism*: it is the use of the internet through a computer or wireless device to conduct violent acts that cause a threat, intimidation, loss of life, or bodily harm, in order to perform political, economic, or social objectives.
- *Cybervandalism*: it includes both *computer vandalism* that destroys the physical computing resources using malicious programs and *data vandalism* that damages someone's account and data through editing the data into something embarrassing or absurd.
- *Computer hacking*: it is a skill for modifying computer software and hardware functions to perform an objective outside the creator's original aim. The aims of hacking include the presentation of hacker skills to steal, update, and destroy data for social, economic, or political reasons. Recently, some organizations hire hackers to hack and fix security vulnerabilities in their systems. The computer hackers are classified into four main types:
  - *White hat* or *ethical hackers*: they include hackers who hack the systems to determine the vulnerabilities in the system security and report to the organizations to take preventive procedures for protecting the systems from any external hackers.
  - *Black hat* or *crackers*: they include persons having bad intentions for hacking the systems. Crackers attack systems through the vulnerabilities or loopholes in the security system and exploit the system for personal, organizational, social, political, or economic benefits.
  - *Grey hat*: they include persons who search for and find out the security vulnerabilities for an organization and then contact the organization's site administrator to submit an offer for solving and fixing this security gap by a specific cost.
  - *Blue hat*: this refers to outside computer security consulting companies that work to test a system prior to its launch, looking for what they can exploit to make it closed. This term also refers to the security professional invited by Microsoft to find vulnerabilities in Windows OS.
- *Cyberstalking*: it is the use of the internet or other electronic devices to stalk or harass individuals, groups, or organizations. This behavior includes false accusations, threats, and stalking.
- *Cybersquatting*: also called domain squatting, it is acting for registering or using an internet domain name with a bad intent for profiting from the goodwill of a trademark belonging to someone else.
- *Creating and distributing viruses over the internet*: the spreading of viruses may cause business damage and financial loss to an organization. These damages and losses include the cost of fixing the system and the salaries of workers during the system's interruption.
- *Cross-site scripting*: it is an unethical process involving the injection of a client site with malicious code script, and when the browser is running, the injected code can access client sensitive information and send it to the attacker servers.
- *Data diddling:* it is a process of changing data before its entry into the computer, often done by a data entry employee or a virus program. Computerized processing of the changed data results in a fraudulent benefit. In most cases, the updated data is changed back after the processing to hide the process.
- *Denial of service attack*: in this cybercrime, the cloud network is overloaded with many unknown processes and often collapses by flooding it with invalid traffic and therefore preventing the correct network traffic.
- *Email spoofing*: it is a process of creating an email message with a forged sender address. It is used in phishing and junk mail campaigns because people do not doubt opening an email when they think it has been sent by the correct sender.

- *Internet time theft*: it refers to hacking the username and password of an organization or individual and using the internet in their place.
- *Logic bombs*: they are part of malicious codes inserted by hackers into system programs that will run some malicious functions according to specified conditions. For example, a hacker may insert code into an active system program, and this code starts to delete some important records at a specified date.
- *Spamming*: it is the use of messaging systems to send unwanted messages called spam (especially for advertising) and also sending repeated messages on the same site.
- *Phishing*: it is a process of stealing sensitive data of an organization or individual via email by disguising as a trusted person in an email. The goal of phishing is to steal personal information such as ID, username, password, and credit card number. The hacker could use this information for stealing money from the user's account. The term *Vishing* (for voice phishing) refers to the use of a mobile phone for stealing user ID, while *SMiShing* refers to the use of SMS for luring and stealing customers.
- *Web jacking*: it refers to hacking an organization by gaining access to its website and either blocking or updating it to serve political, social, or economic intentions.

4. Cybersecurity for ICT systems

Recently, experts, computer professionals, and IT policymakers have expressed increasing attention about securing and protecting information and communications technology (ICT) systems from cyberattacks. They are expecting the increase of number, strength, and effect of cyberattacks over the next ten years. The act of protecting ICT systems and their resources is called *cybersecurity* [21].

Therefore, cybersecurity is defined as "*the practice of protecting systems, networks, and programs from cyberattacks*". These cyberattacks are mainly for accessing, updating, and destroying sensitive data, extorting money from users, or damaging business processes. Developing an effective cybersecurity methodology is particularly challenging because attackers are becoming more motivated and innovative. In some discussions, there is unacceptable confusion between cybersecurity and other security concepts such as privacy, data sharing, and data monitoring. *Privacy* refers to the ability of an individual to isolate himself or control his information so that it is not accessed by others, thereby expressing himself selectively. Therefore, cybersecurity could help protect privacy in the cloud computing environment and for protecting against undesired monitoring as well as for gathering intelligence from a cloud system [22].

5. DoS and DDoS cybersecurity attacks

The main objective of the denial of service attacks is to infect computer resources by overloading the web-based services (*e.g.*, user website, user webpage, etc.) with traffic. The hacker's goal is to deactivate the web service of the target machine or network and prevent authorized users from accessing their services. The hacker uses a large number of machines to publish the attacks by overloading the network of the target organization [23]. The DDoS attacker aims to flood cloud resources by numerous hacking requests to prevent authorized users from executing their services.

On the other hand, in DoS attacks, the hackers inject malicious code into an active website for target organizations through the web browser, and as a result, it prevents legitimate users from accessing their cloud services successfully. DDoS attacks are normally worse than DoS attacks because DDoS hackers overload the target cloud system with numerous web service requests in order to suspend the target network.

Most of the dangerous attacks targeting cloud security come from DDoS, especially from HTTP and XML-based DDoS attacks. Due to the vulnerability in a certain part of the cloud interface, DDoS attacks are easy to execute and very difficult for security experts to discover [24]. The DDoS attacks are usually published from multiple computers, while DoS attacks are published from a single computer. Really, these computers (called *botnet*) are not all owned by the hackers, but they are added to the hacker’s network by malicious software and intended to damage or disable computer networks.

5.1 Types of cyber-DDoS attacks

The cloud computing attacks not only try to infect the user cloud infrastructure but also try to infect user services. It is very hard to identify the different types of DDoS attacks by using one measure because the hackers publish each attack with different features, and each one belongs to multiple categories. We classified the DDoS attacks into three categories including *volume-based*, *protocol-based*, and *application layer-based attacks.*

5.1.1. Volume-based attacks

In volume-based attacks, the attackers overload the targeted computer by a large set of junked data. This process consumes network bandwidth (volume) and other cloud resources. This category includes the *user datagram protocol* (UDP) floods *and internet control message protocol* (ICMP) floods [25]:

- *UDP floods*: they are a simple connectionless protocol, in which the header part consists of a source port attribute, a destination port attribute, a header checksum part, and a length attribute that specifies the length of the entire packet specified by bytes. The port numbers are used for determining the application to which the packet data should be directed. The attacker targets and overwhelms random ports on the host with IP packets containing UDP packets using *zombies'* machine. The host looks for applications related to these datagrams. When none are found, the host issues a "destination unreachable" packet back to the sender. The cumulative effect of being bombarded by such a flood is that the system becomes overloaded and therefore unresponsive to valid traffic.
- *ICMP floods*: they are a connectionless protocol used to send reports and messages for IP operations, diagnostics, and errors. In the ICMP flood attacks, hackers saturate the target machine by sending numerous and continuous ICMP request packets that make the bandwidth utilization reach its maximum value. As a result, the attack prevents the target machine from responding, and the users cannot access their services via the cloud.

5.1.2. Protocol-based attacks

The attackers exploit the gaps related to various network protocols and infect the network by overloading the target's resources. This category includes the *SYN floods*, *ping of death*, and *smurf attack* [25].

- *SYN floods*: the TCP connection starts with a three-way handshake called SYN, SYN-ACK, and ACK. The connection between the authorized user and the server is achieved by sending a connection request from the user to the server in the form of a synchronization message (SYN). When the server acknowledges the received SYN message, it sends back SYN-ACK requests to the user. Finally, the connection is confirmed by an ACK request from the user to the server. When the hacker sends a large number of IP packets to the server to flood the cloud services, passing through the three-way handshake causes SYN flooding attacks. Also, SYN flooding can be done by sending packets with a rigged IP address [26].
- *Ping of death*: this attack occurs when the hacker sends an IP packet with a size larger than 65,535 bytes (*i.e.*, larger than the maximum size of the normal IP protocol). The processing of an oversized packet will affect the target computers connected to the networks and also affect the performance of other network resources. When the oversized packet is recollected, the target system will crash and the performance of the cloud environment will be affected.
- *Smurf attack*: it is a form of a DDoS attack that causes packet overflow on the victim machines by using ICMP protocols. When publishing, large packets are generated by hackers using a "*spoofing*" technique. The phony IP address that is attached to these packets becomes the victim, as their IP is flooded with traffic [27].

5.1.3. Application layer-based attacks

This attack targets particular web applications and focuses on specific vulnerabilities that prevent the application to deliver web services to the user. It includes the HTTP and XML DDoS attacks:

- *HTTP-based DoS attacks*: when the clients use the cloud system through an internet browser, they will send requests by two main ways: GET and POST. This will be done through an HTTP server. For normal links, a GET request will be used. The GET request aims to retrieve a static piece of data, and the URL focuses on this data. The GET request is executed when you type a URL. POST requests are used when clients use a Forms GUI. A POST request uses parameters, which usually take their values from the input fields. The attacker infects the target server by sending many requests until the computing resources become overloaded. As a result, the victim machine becomes unable to process the correct request. Since POST requests include parameters, they usually become more infected than GET requests when processed on the server [8]. The HTTP GET and POST request messages are used by the hackers to target the server of an organization. The HTTP GET request gets some information from the server, and when the server is overloaded with rigged GET requests that used the CPU and RAM, hence the target server will be unavailable to reply to any other requests. On the other hand, the HTTP POST processes input

data through Forms GUI interface that requires more computation from the server. Therefore, the HTTP POST-DDoS attacks are more dangerous than the GET-DDoS attacks [28].

- *XML-based DoS attacks*: the majority of information technology workers and specialists in the field of cloud computing agree that security is the main concern for SOA (*service-oriented architecture*) and XML messages. It is realized that SSL (*secure sockets layer*) is limited by its lack of content security and reliability. One of the problems that face the use of XML-based web services is that they remove some network security which causes DDoS attacks transmission through the internet to the target server [8]. Another objective of XML DoS attacks is to overload the network resources by random requests while handling SOAP (*simple object access protocol*) messages [29].

6. The proposed cybersecurity approach

In spite of the performance and capability of cloud security, in some cases, the cloud infrastructure responds to the DDoS attacks, which causes the unavailability of the target services and crashes software applications used by the cloud servers. As shown in Fig. 1, the researcher introduces the new cybersecurity model of the proposed approach that used for detecting and preventing cloud services and systems against DDoS attacks. The system prototype was implemented and used for protecting cloud-based career and educational guidance systems against DDoS attacks.

The proposed algorithm starts with handling the client IP request through the *Request_controller* process used to check the server availability. If the server is not available, then the system calls the *Unavailable_requests* process and returns back to the client site; otherwise, the server executes the client request. The detection against known attacks is checked for the IP request through the *Attack_IP* process. If there is a positive response for an attack, then the system calls the *Blacklist_IP* process to store the record in *blacklist_IP* database table; otherwise, the IP request passes as input into three DDoS detectors as follows: (1) UDP ICMP detector that checks and ignores any IP packet containing UDP or ICMP request packets sent by random zombies' machine and maintains the bandwidth utilization size; (2) SYN_PingOfDeath_Smurf detector that accepts only IP packet less than the max size of the IP protocol, processes it through valid three-way handshake of SYN, SYN-ACK, and

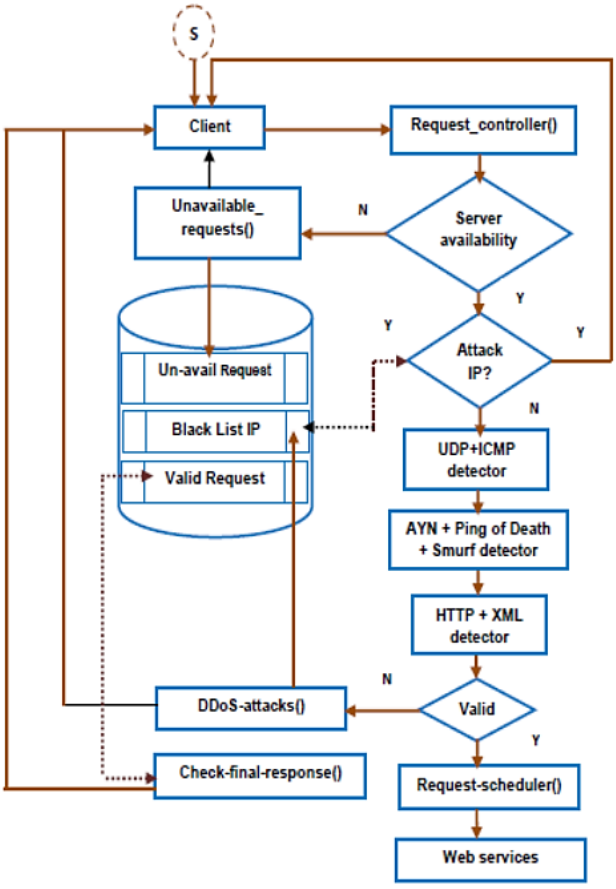

Figure.1 The structured design for our proposed approach

ACK, and deletes any ICMP echo requests from a rigged IP address; and (3) HTTP_XML detector that tests the input IP packets against both HTTP and XML DDoS attacks. If the input IP is not valid, then the DDoS_*Attacks* process is executed which sets some flags related to the source attack and stores the requested IP address as a blacklist attribute value in the *blacklist_IP table*. In case of a valid IP address, the system calls the *Request_scheduler* process, schedules the IP address, handles the request, and stores the valid IP request in the *Valid_request* table. The *Web_services* process is executed only on the valid IP. Finally, the *Check_final_response* process is executed to check the final response, removes the processed request from the *Valid_request* table, and sends an acceptance message to the *client* site.

6.1 The proposed algorithm

The researcher measured the performance of the proposed algorithm in terms of *accuracy, sensitivity, and specificity* using the following formulas:

$$Alg_{acc} = (NT_p+NT_n)/(NT_p+NT_n+NF_p+NF_n) \times 100\%$$

$$Alg_{sen} = (NT_p) / (NT_p + NF_n) \times 100\%$$

$$Alg_{spe} = (NT_n) / (NT_n + NF_p) \times 100\%$$

Where NT_p is the number of correct cases, set as attacked packets in the experiment; NT_n is the

number of correct cases, set as normal packets; NF_p is the number of incorrect cases, set as attacked packets; and NF_n is the number of incorrect cases, set as normal packets.

Algorithm: Securing cloud services against DDoS attacks

```
1.   Get new.client.request()
2.   Request_controller()
3.   if ( Not(Server.availability(); ) then
4.      { Unavailable_requests();
5.        Goback_client_site();}
6.   else if ( attack_IP(client.request.IP) ) then
7.      {  Insert_into_blacklist_IP();
8.         Goback_client_site();}
9.   else
10.     {Call  UDP_ICMP-detector;
11.      Call  SYN_Pingofdeath_smurf_detector;
12.      Call HTTP_ XML_detector; }
13.  If  (Not(Valid.client.request)) then
14.      { DDoS_attach();
15.        Insert_into_blacklist_IP();
16.        Goback_client_site();}
17.  else
18.      Request_scheduler();
19.      Web_services ();
20.      Check_final_response()
21.      Insert_into_valid_request_table();
22.      Process.client.request();
```

7. Experimental results and evaluation

The author used the cloud-based career and educational guidance system as a case study with different experimental data sizes and thresholds to get efficient results of the proposed approach [30].

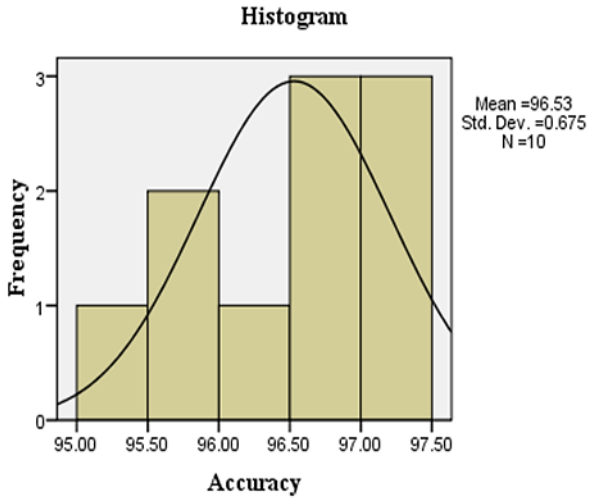

Figure.2 The performance measure of system' accuracy

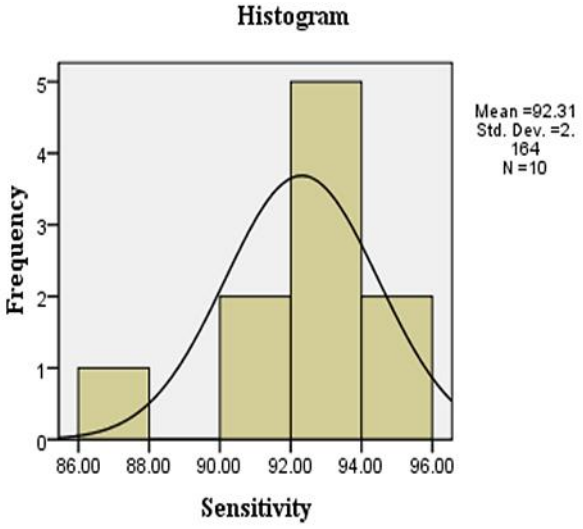

Figure.3 The performance measure of system' sensitivity

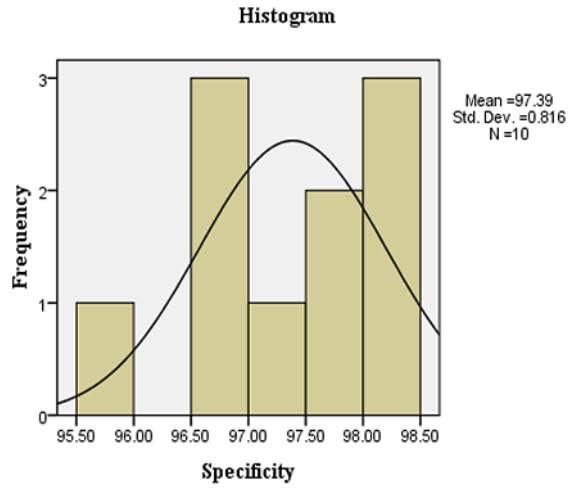

Figure.4 The performance measure of system' specificity

The effectiveness of our approach under multiple source attacks tested in terms of accuracy, sensitivity, and specificity. The researcher used ten random data sizes of IP packets and ten thresholds (K=10), where K <= NT_p. The proposed algorithm was applied using various inputs; **i**n addition to NT_p, NT_n, NF_p, and NF_n, two important fields (the source IP address and the destination IP address) were considered.

Table 1 shows the results of using the proposed approach and algorithm for detecting and preventing DDoS attacks. The researcher concludes that the system has an average performance of 95.41%, an average accuracy of 96.53% as shown in Fig. 2, an average sensitivity of 92.31% as shown in Fig. 3, and an average specificity of 97.39% as shown in Fig. 4.

As a result, the proposed approach can also be implemented in large-scale cloud-based systems

Table 1. Performance evaluation results

Protecting cloud computing services against DDoS attacks								
N	K	T_p	T_n	F_p	F_n	Accuracy	Sensitivity	Specificity
1000	155	330	670	30	20	95.24%	94.29%	95.71%
2000	200	400	1600	55	30	95.92%	93.02%	96.68%
3000	240	600	2400	62	35	96.87%	94.49%	97.48%
4000	280	710	3290	72	55	96.92%	92.81%	97.86%
5000	330	830	4170	88	70	96.94%	92.22%	97.93%
6000	390	570	5430	98	83	97.07%	87.29%	98.23%
7000	450	890	6110	120	95	97.02%	90.36%	98.07%
8000	530	1500	6500	126	105	97.19%	93.46%	98.10%
9000	640	3100	5900	190	211	95.73%	93.63%	96.88%
10000	750	3400	6600	210	315	96.40%	91.52%	96.92%
Performance average						96.53%	92.31%	97.39%

(such as a health cloud system), as well as in smaller cloud systems (such as private cloud systems for small and medium-sized organizations).

7.1 Correlation analysis for validating the proposed approach

The author used correlation coefficient analysis to validate the effectiveness of the proposed approach and to identify the relationship between malicious and legitimate traffic. The research study presented the performance of the proposed approach, and its efficiency was determined by the suitable data size. The proposed approach was described in terms of correlation coefficient analysis as follows:

The study assumed that *n* IP packets are checked in each time interval T_l. For each feature, we obtain *n* values.

Inputs: F-sample of network traffic,

$$f_i^l = (f_i^{l,1}, f_i^{l,2}, \dots, f_i^{l,n}),$$
$$f_j^l = (f_j^{l,1}, f_j^{l,2}, \dots, f_j^{l,n}) \quad (1)$$

Where $f_i^{l,n}$ is the value of f_i in the n^{th} observation during the l^{th} time interval t_l.

For each sample f_i^l and f_j^l:

1. Compute $f_i^{l\prime} = \frac{\Sigma(f_i^l)}{n}$, and $f_j^{l\prime} = \frac{\Sigma(f_j^l)}{n}$
2. Compute the sample variances of f_i^l and f_j^l as: $D^2(f_i^l)$, and $D^2(f_j^l)$, where;

$$D^2(f_i^l) = \frac{\Sigma(f_i^l - f_i^{l\prime})^2}{n-1}, D^2(f_j^l) = \frac{\Sigma(f_j^l - f_j^{l\prime})^2}{n-1} \quad (2)$$

3. Compute the covariance of f_i^l and f_j^l as:

$$cov(f_i^l, f_j^l) = \frac{\Sigma(f_i^l - f_i^{l\prime})(f_j^l - f_j^{l\prime})}{n-1} \quad (3)$$

4. Compute the correlation coefficient of f_i^l and f_j^l as:

$$r(f_i^l, f_j^l) = \frac{cov(f_i^l, f_j^l)}{\sqrt{D^2(f_i^l) \times D^2(f_j^l)}} \quad (4)$$

5. *If* $(r(f_i^l, f_j^l) \geq \delta)$
   {*call* alarm-attack-msg();
   call insert-blacklist-IP();}
   else
   {*call* insert-valid-request-table();
   call client.request();
   call get_next_ IP();}

The correlation coefficient $r \in [-1, 1]$ measures the direction and strength of the relationship between the network traffic types f_i^l and f_j^l. *r* represents the *direction*, and the magnitude indicates the *strength* of the relationship.

8. Conclusions

The research aims to introduce and discuss a new cybersecurity approach for detecting and preventing

cloud services and systems against all types of DDoS attacks such as volume-based, protocol-based, and application layer-based DDoS attacks. The researcher proposed a new algorithm for implementing the proposed approach. The performance and effectiveness of the proposed algorithm were evaluated in terms of accuracy, sensitivity, and specificity. The researcher also used correlation coefficient analysis to validate the effectiveness of the proposed approach and to identify the relationship between malicious and legitimate traffic, to distinguish the contribution of the research for preventing DDoS attacks. The research used the implementation of the cloud-based career and educational guidance system as a case study with various experimental data sizes to evaluate the proposed approach. The results of the experiments were highly promising for detecting and preventing DDoS attacks. The research evaluation concluded that the average performance was 95.41%, the average accuracy was 96.53%, the average sensitivity was 92.31%, and the average specificity was 97.39%.

Acknowledgments

The author extends his appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through General Research Project under grant number (GRP-35-40 /2019).

References

[1] H. El-Sofany, A. Al-Tayeb, K. Alghatani, and S. El-Seoud, "The Impact of Cloud Computing Technologies in E-learning", *International Journal of Emerging Technologies in Learning* –iJET, Vol. 8 iS1, pp.37-43, 2013.

[2] NIST , "Final version of NIST cloud computing definition published", *National Institute of Standards and Technology's*, pp. 1-7, 2018 http://www.nist.gov/itl/csd/cloud-102511.cfm

[3] P. Jain, D. Rane, and S. Patidar, "A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment", In: *Proc. of the 2011 World Congress on Information and Communication Technologies*, pp. 456–461, 2011.

[4] B. Gowrigolla, S. Sivaji, and M. Masillamani, "Design and auditing of cloud computing security", In: *Proc. of the 2010 5th International Conference on Information and Automation for Sustainability*, pp. 292–297, 2010.

[5] J. McKendrick, "Cloud divide: senior executives want cloud, security and IT managers are nervous", http://www.zdnet.com/blog/serviceoriented/cloud-divide-senior-executives-want-cloud-security-and-it-managers-are-nervous/6484, pp. 1-7, 2011.

[6] P. Chouhan, and R. Singh, "Security Attacks on Cloud Computing With Possible Solution", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 6, No. 1, pp. 92-96, 2016.

[7] C. Babcock, "9 Worst Cloud Security Threats", *InformationWeek*,https://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085, pp. 1-6, 2018.

[8] K. Santhi, "A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, pp.416-420, 2013.

[9] R. Deshmukh and K. Devadkar, "Understanding DDoS Attack & Its Effect In Cloud Environment", In: *Proc. The 4th International Conference on Advances in Computing, Communication and Control*, pp. 202–210, 2015.

[10] CSA, "The Notorious Nine Cloud Computing Top Threats in 2013", *Cloud Security Alliance Journal*, https://downloads.cloud securityalliance.org/initiatives/topthreats/TheNotoriousNineCloudComputingTopThreatsin2013.pdf, pp. 1–21, 2013.

[11] R. Sarhadi, and V. Ghafori, "New Approach to Mitigate XML-DOS and HTTP-DOS Attacks for Cloud Computing", *International Journal of Computer Applications*, Vol. 72, No.16, pp. 27–31, 2013.

[12] CERT Advisory, "Smurf IP Denial of Service Attacks", http://www.cert.org/advisories/CA-1998-01.html, pp. 1–78, 1998.

[13] S. Padmanabhuni, V. Singh, K. Senthil, and A. Chatterjee, "Preventing Service-Oriented Denial of Service (PreSODoS): A Proposed Approach". In: *Proc. IEEE International Conference on Web Services*, pp. 1–8, 2006.

[14] A. Chonka,Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks", *Journal of Network and Computer Applications*, pp. 1097- 1107, 2010.

[15] A. Bonguet, and M. Bellaiche, "*A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing*", *Future Internet Journal*, Vol. 9, No. 43, pp. 1-19, 2017.

[16] M. Masdari and M. Jalali, "A survey and taxonomy of DoS attacks in cloud computing Secur", *Commun. Netw Journal*, pp. 3724–3751; SCN-15-0746.R1, 2016.

[17] O. Osanaiye, K. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework", *J. Netw. Comput. Appl*, Vol 67, pp 147–165, 2016.

[18] H. El-Sofany, I. Taj-Eddin, and S. El-Seoud, "A case study of the Impact of Denial of Service Attacks in Cloud Applications", *Journal of Communications (JCM)*, Vol. 14, pp. 153-158, 2019.

[19] J. Julian, S. Nepal, and Y. Guo, "Cybersecurity threats in cloud computing", *Australian Journal of Telecommunications and the Digital Economy*, Vol .1, pp. 1-17, 2013.

[20] J. Pande, "Introduction to Cyber Security", *School of CS & IT, Published By: Uttarakhand Open University, Haldwani*, pp. 1-152, 2017.

[21] Cisco, "What is cybersecurity?" https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html, pp. 1-5, 2019.

[22] E. Fischer, "Cybersecurity Issues and Challenges: In Brief", *Congressional Research Service*, Vol. 7-5700, pp. 1-12, 2016.

[23] Wikipedia,"Denial of service attack", https://en.wikipedia.org/wiki/Denial-of-service_attack, 2019.

[24] T. Karnwal, T. Sivakumar, and G. Aghila, "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack", In: *Proc. of the 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, pp. 1–5, 2012.

[25] V. Vidhya, "A Review of DOS Attacks in Cloud Computing", *Journal of Computer Engineering*, Vol. 16, pp.32-35, 2014.

[26] M. Kumar, A. Panwar, and A. Jain, "An Analysis of TCP SYN Flooding Attack and Defense Mechanism", *International Journal of Engineering Research & Technology (IJERT)*, Vol. 1, No. 5, pp. 1–6, 2012.

[27] B. Prabadevi, and N.Jeyanthi, "Distributed Denial of Service Attacks and its effects on Cloud Environment- a Survey", *IEEE Explore*, pp.1-5, 2014.

[28] G. Jaafar, S. Abdullah, and S. Ismail, "Review of Recent Detection Methods for HTTP DDoS Attack", *Journal of Computer Networks and Communications*, Vol. 2019, pp. 1-10, 2019.

[29] A. Vinayakrao, N. Shekokar, and M. Maurya, "The Countering the XDoS Attack for Securing the Web Services", *International Journal of Computer Science and Information Technologies*, Vol. 5, No. 3, pp. 3907-3911, 2014.

[30] H. El-Sofany, and S. El-Seoud, "A Cloud-based Educational and Career Guidance Model using Fuzzy Logic Concepts", In: *Proc. the 2nd International Conference on Network Technology, and 8th International Conference on Software and Information Engineering*, pp. 167-172, 2019.

[31] C. Amita, M. Nitish, K. Harish, and K. Sakshi, "Analysis of DDoS Attacks in Heterogeneous VoIP Networks: A Survey", *International Journal of Innovative Technology and Exploring Engineering*, Vol. 8, Issue-6S3, pp. 242-246, 2019.

[32] K. Naveen, M. Nitin, and N. Yogendra, "Isolation of Distributed Denial of Service Attack using Threshold Based Technique in Internet of Things", *International Journal of Recent Technology and Engineering*, Vol. 8, Issue-1C2, pp. 87-93, 2019.