Performance Analysis of an Effective Approach to Protect Cloud Systems Against Application Layer Based Attacks

https://doi.org/10.3991/ijoe.v15i03.9931

Hosam F. El-Sofany
King Khalid University, Abha, Kingdom of Saudi Arabia
Cairo Higher Institute for Engineering, Cairo, Egypt

Samir A. El-Seoud(✉)
British University in Egypt, Cairo, Egypt
Samir.elseoud@bue.edu.eg

Abstract—Cloud computing is a new paradigm for hosting hardware and software resources and provides a web-based services to organizations and consumers. It also provides an easy to use and on-demand access to cloud based computing resources that can be published by easy, minimal administration and with a great efficiency. Services of cloud computing are accessing and sharing through internet connection thus it is open for attacker to attack on its security. Application layer based attacks is one of Distributed Denial of Service attacks (DDoS) that can cause a big problem in cloud security. The main objective of DDoS attacks is to infect computer resources (e.g., software applications, network, CPU, etc.) and make them not working properly for the authorized users. In DDoS, the attacker tries to overload the web-based service with traffic. HTTP and XML-based DDoS attacks are founded under the application layer based category of DoS attacks. This category of attack is focused on particular web applications. The main objective of this research paper is to introduce an effective approach to protect cloud-based systems against application layer based attacks. Complexity analysis, effectiveness and performance evaluations of the presented approach are presented. The feedbacks of the experimental results were highly promising, for protecting cloud computing systems against both DoS and DDoS attacks. Correlation analysis model is also used to validate the efficiency of the proposed approach.

Keywords—Cloud computing, cloud security, cloud attacks, denial of service attacks, distributed denial-of-service attacks, correlation analysis.

1 Introduction

With the continuous development of internet, hardware and software, cloud computing became the most important issue for organizations. Cloud computing providers use the Internet as basic, and essential communications tool to deliver their IT re-

sources to their contracted organizations on a pay-as-you-use basis [1]. Cloud computing architecture consists of three service layers called:

- SaaS (Software as a service)
- PaaS (Platform as a service)
- IaaS (Infrastructure as a service).

Therefore, Cloud computing model is viewed as 5 components that include: *clients, platforms, applications, infrastructure* and *servers*. Cloud model supports availability and is consists of 5 essential characteristics that provide

- High scalability and elasticity
- Availability and reliability
- Performance and optimization
- Accessibility and portability
- Manageability and interoperability

The current cloud computing models are published in one of the following 4 deployment models:

- **Private cloud:** In this model, the cloud infrastructure is provided for private used by many users working in single organization.
- **Community cloud**: In this model, the cloud infrastructure is provided for specific use by a specific community of consumers from organizations that have shared concerns (i.e., mission, security requirements, policy, and compliance considerations)
- **Public cloud:** In this model the cloud infrastructure is provided for open use by general public
- **Hybrid cloud**-In this model the cloud infrastructure is composite of 2 or more cloud infrastructures [3, 4]. Cloud deployment models with their internal infrastructure are shown in Figure 1.

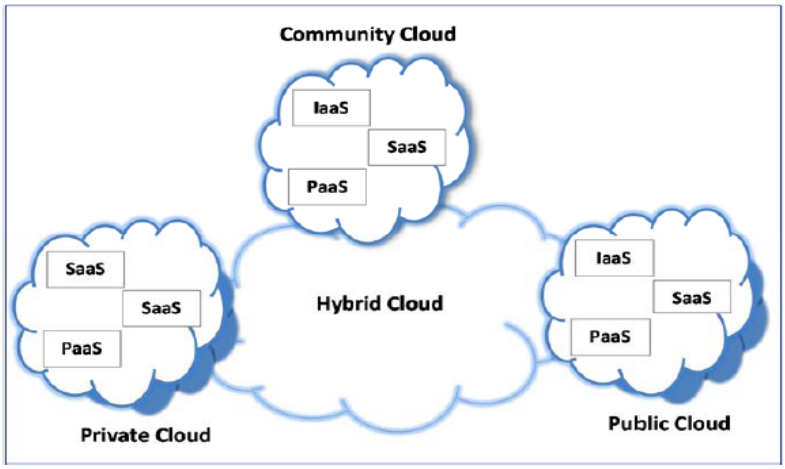

Fig. 1. Distribution of cloud deployment models and their infrastructure

1.1 Cloud computing Security

Is critical when developing cloud applications and services. Cloud security problems are arise because the customer data, information, and programs are stored in the servers of cloud provider [5]. Cloud computing security identifies some important objectives:

- **Availability:** Services should be always available for users at any time, and at any location. Cloud providers should protect cloud-based systems from attacks to reduce or prevent end-user security vulnerabilities.
- **Authentication:** The identity of individuals involved in the web communication should be assured
- **Accountability:** In which the cloud computing systems ensure that no individual can deny its sharing for data transfer between them.
- **Confidentiality:** User's data should be secret in the cloud systems by making it available only to authorize individuals and prevent access for unauthorized individuals.
- **Integrity:** In which the cloud-based systems ensure that data has not been changed in any way while it is maintained or while its processing and transfer through the cloud networks.
- **Portability**: Support portability such as *Postal Service* that can take action to change Continuity of Operations (CPs) when required to satisfy *availability*, *confidentiality*, and *integrity* requirements. This includes the ability to close an account for a particular time and date and to copy data from one CP to another.

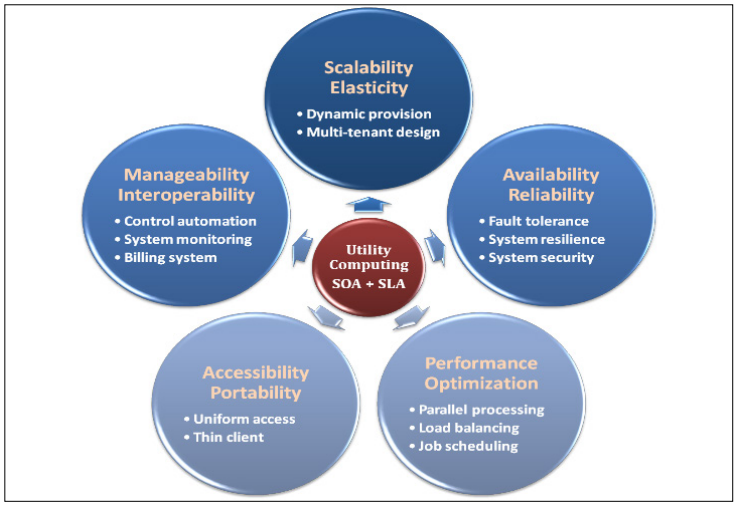

Fig. 2. Five essential characteristics provided by cloud computing

The above security objectives require; use of modern security mechanisms and services to be developed, for improving cloud-computing security.

- A **Security Mechanism** can be identified as "a process which aimed to detect or/and prevent a security attacks".
- A **Security Service** can be defined as "a processing service that aim to improve and support the security of data and information transfers of an entity". Security services assist in countering security attacks [6]. Since cloud systems using and sharing large amount of data, information, and services. So, the goal of attackers is to destroy or steal customer resources. They are exploit the vulnerabilities related to cloud environment.
- In **DoS Attacks**, the attacker tries to overload the target machine with web service requests so that it cannot reply to any other requests and hence as the result, the resources will be unavailable to the authorized users. On the other hand, in *DDoS attacks*, the attacker uses several compromised computers called *zombies* to launch DoS attack on the target machine, and as a result service will be delayed or/and stopped [7, 8]. DDoS attacks are frequently increasing and target cloud-computing systems. This issue opened many research areas and motivated the authors to study the problem and to innovate a proper approach to protect the cloud against this type of attacks.

The paper is consists of five sections as following: in section two, we present some related and previous research work done in the same area. In section three, we present denial of service attacks categories and description. In section four we introduce the proposed approach to protect cloud-computing applications against application layer based attacks. The performance analysis via experimental results of the proposed approach and complexity analysis of the proposed algorithm are also presented. The paper concluded in section five.

2 Related Work

Recently, cloud computing has been greatly used in various areas include scientific and academic research, industry technology and organization development. [9]. By using *web services* in cloud computing we will lead to get one of the dangerous attacks of cloud based systems which produces from HTTP Denial of Service or XML-based Denial of Service attacks. These two kinds of attacks are easily executed but several times very difficult to be detected. DDoS attack is one of the security threats that challenge the availability of cloud computing systems [10]. Many research studies have been published in the area of *network security* but security of cloud computing is still new and challengeable. In the cloud-computing field, most of the research studies are moving towards to cloud computing security. Every day we remember that cloud computing security is having many related problems according to new machines vulnerability and exists of several example in which cloud based systems is enduring new attacks [11].

From the previous research, studies we can conclude that from many cloud attacks there are 15%-20% are DoSs attacks. Websites for yahoo's organization were affected

by Distributed Denial of Service attacks (in 2000). Web portal for grc.com was targeted by series of DDoS (in May, 2001). The business transactions of these companies were affected negatively, as a result of these DoSs attacks. The following experimental results from the study conducted by VeriSign and Forrester companies in (March 2009) are presented, to show and analyze the impact of DDoS attacks and its infections and defense. The survey was conducted among four hundred respondents from the United State and Europe [12].74% had infected by one or more DDoS attacks in their organizations. From this 74%, there are 31% of DoSs attacks caused service stop, there are 43% of DoSs attacks does not result to stop the services. The concluded result of the conducted survey of DoS attacks in cloud computing is: as the use of cloud computing based systems increases the percentage of DDoS attacks will also increase. In Cloud computing networks when the access work increases by users on a service, it will start providing computational power to support the additional load. This means that cloud system works against the attacker, but to some extent it assists the attacker by give him the authority to do most possible denial on availability of service. The authors in [12] have introduced a cloud defender application system called CSQD (Cloud Service Queuing Defender", for detecting and mitigating XML vulnerabilities in web-based services. One of the related works in cloud security defense is published by Ashley Chonka et al. [13]. The authors in this paper have presented a protector-based on neural network for detecting and filtering DOS attacks and also introduced a solution for discovering attacks in the basis of trace backing. They have implemented the solution according to their previous research study on SOTA, which was based on service-oriented and service-oriented network architectures.

The researchers in [14] have proposed a framework called "Preventing Service Oriented Denial of Service" that used for detecting and preventing XML based DoS attacks on Web services based systems. The proposed paradigm relies on content introspection to detect any XML-DoS attack. They used a Patricia Trie based model representation so that the schemas and the request messages can be compared and validated in a performance efficient way.

In [15], the authors have presented a comprehensive survey study on DoS and DDoS attacks and defenses in cloud computing paradigm. The research study of XML and HTTP DoS allowed for showing most of the available defences. The authors have evaluated the DoS and DDoS protection and defense with appropriated experimental model. They have introduced a research results to help cloud providers for defining the SLAs (Security Service Level Agreements) as "the protection of the fundamental security attributes" through the definition of *confidentiality*, *integrity* and *availability*.

The researchers in, [16] have presented a research study of DoS attack type against virtual machines and hypervisors in cloud environment. On other hand the authors enumerate a well-known network defense and cloud computing defense against DoS attacks.

The authors in [17], have presented a survey for DDoS attacks that infecting cloud computing systems. They categorized the attacks into app-bug level and infrastructural level and presented the different tools for conducting these attacks.

The Cloud Computing models require innovative methods to protect the users and their related resources such as (data, information, applications, services, etc), on other hand to protect the cloud computing provider infrastructure. As presented above, cloud-computing security is now a good and hot area for research and innovation.

The researchers in [25] have proposes a system for detecting and preventing XML and HTTP based DoS attacks. The Efficiency and performance of the system is computed and evaluated. The feedbacks of the experimental results were highly promising, for detecting and preventing both DoS and DDoS attacks. The evaluation shows encouraging results with performance average of (94.73%) for detecting DoS attacks, and (93.48%) for detecting DDoS attacks.

In this research study, we improve the proposed mechanism introduced in [25] to protect cloud-computing systems against application layer based attacks.

3 Denial of Service Attacks Categories and Description

The main goal of the DOS attacks is to target and infect cloud resources such as (software applications, network, CPU, databases, communication link, etc.). Dos attack causes serious damages for cloud services, so it is essential to develop a detection mechanism for protecting cloud computing services.

The DOS attack is usually published from a single computer, as opposed to a DDOS attack, which is published from multiple computers. Naturally these computers aren't all owned by the attacker. These computers are usually added to the hacker's network by means of *malware.* This group of computers is called a *botnet*. As the attack may be distributed over multiple computers, it will be very hard to differentiate authorized users from attackers. DDOS attacks are normally worse than DOS attacks. The attacker goal is to disrupt the web service or network access in order to stop authorized users from accessing to his service. The attacker targets to use large number of machines to infect them by DDoS attacks, through overload of network and CPU [18]. This will be done in the absence of any good mechanisms for facing DDoS attacks. Also, in DoS attacks, an attacker tries to inject malicious instructions into active web site via the current web browser by opening many windows and that make the access of authorized user to the cloud services is denied. In addition, an attacker tries to overload the target cloud based apps with service requests in order to stop or failure responding to any new requests and hence made resources unavailable to authorized users. It is difficult to distinguish the different types of DoS and DDoS attacks by using only one measure because each type of attack has different features that may suggest it belongs to multiple classes. Table 1, Shows the different attack categories, the description of each category, and DoS attack types under each category [25].

Table 1. DoS attack categories, description, and types of each category.

Attack category	Description	DoS attack types under each category	
Volume (bandwidth) based	The attacker tries to increase the load on the victim	UDP floods Or User Datagram Protocol-	In this type, the attackers send randomly many user datagram protocol packets to target ports of the target cloud apps using zombies com-

attacks	computer with large amounts of infected data, this action will consuming the cloud network bandwidth and other cloud resources [20].	floods	puters and when the target cloud apps identifies no valid apps on each port, it responds to the spoofed Internet Protocol - IP addresses by generating 'destination unreachable 'ICMP packet.
		ICMP Floods Or Internet Control Message Protocol-floods	In ICMP Floods (or Ping flood) attacks, the attackers saturated the victim machine by sending a lot of ICMP echo request packets and when the infected machine tries to response, the max bandwidth utilization will be reach to max value. As a result, authorized users didn't able to access the cloud network.
Protocol based attacks	The attackers try to gain benefit of the gap associated with various network protocols and target the cloud by overloading the target's resources [20].	SYN Floods	When attacker sends numerous number of packets to the server and infects the cloud service process to complete through the three-way handshake (SYN, SYN-ACK, and ACK.), this will cause SYN flooding attacks. Therefore the server will wait to finish the target process for all packets remained, which causes a strong delay and hence the server unable to process authorized user's requests [21].
		Ping of Death	In this type, the attacker sends an IP packet with a size more than the max size of the IP protocol, (i.e.,> 65,535 bytes). Working with overloaded and big-size packet will affects the victim's computer connected to the cloud networks, and affects other cloud system resources. Recently, the cloud network environment and cloud operating systems are disregard any IP packets > 65,535 bytes.
		Smurf Attack	In this type, the attacker sends a large number of ICMP echo requests from a rigged IP add to a distributed IP add rather to a specific system. These requests are rigged where: source IP add = victim's IP, and IP destination add = distributed IP add [22].
Application Layer based attacks	Most attacks in cloud computing come particularly from HTTP, and XML based DDoS attacks. Due to some vulnerability in the cloud system interface. This attack category is focused on particular web applications, and sends HTTP requests outside the boundary that it can handle [19].	HTTP based DoS Attack (HDoS)	In this type, the attacker try to use the HTTP Get and Post request messages to target and infect the victim computer. One of the objectives of HTTP GET request is to get information from the server, and when the server is overloaded with rigged GET requests that utilizing the memory, then target server will be unable to reply to any further requests and hence it denied the requested service. The HTTP POST request is different than HTTP GET request, because it is involve input data as a parameter through Forms GUI which requires more computation from the server side. As a result we can say that HTTP POST DDoS attack is more danger than GET attacks [8, 23].
		XML based DoS Attack (XDoS)	XML DoS attacks are very asymmetric to transmit the harm to the victim machine. Worse still, DDoS vulnerabilities in code that processes XML are also extremely widespread [8]. One of the main objectives of XML DoS attacks is to overload the network resources of the cloud system while handling SOAP (Simple Object Access Protocol) messages. There are three ways for publishing XDoS attack

			called oversized payload, external entity references and entity expansion [24].

4 The Proposed Approach

In spite of the cloud performance and capability, the cloud infrastructure responds to DDoS attacks, which are most serious threat capable of crashing applications that stored on cloud. In this section, we introduce a proposed approach to protect cloud applications against application layer based attacks.

The proposed approach includes the following main functions that define the system processes. These functions produce system operations and control the constraints on each process. Some of these functions include:

- **Request_controller ():** This process is used to check the "*server availability*"; for "Yes/*No*" responses action.
- **Unavailable_requests():** This process is used to compare the action taken with the last record in the *"unavailable_ requests*" *table* that has taken the server down, and go back to the client site; otherwise the system execute the "*Attack_IP*" validation process.
- **Attack_IP ():** This process is used to check if "Yes" response, then the request is stored as a black list request record in the "*blacklist_IP" table*, and go back to the client site also; otherwise the "*XML_HTTP_DDoS-Detector*()" process is executed.
- **XML_HTTP_DDoS_Detector ():** This process is used to validate the request against the XML and HTTP DDoS attacks. If the request is not valid (*i.e.*, *No* response); then the system run the "*XML_HTTP_Attacks* ()*"* process.
- **XML_HTTP_ Attacks ():** This process adds some flags in the request's header, these flags is used to find source of attack in the next executions, and then stores a request IP address as a black list request record in the "*blacklist_IP" table*, and go back to the client site; otherwise (*i.e.*, in case of valid request) the system schedules the request through the "*Request_scheduler*" process.
- **Request_scheduler ():** This process is used to store the valid request in the temporary database table "*valid_request"*, if a request is put in the "*valid_request"* table, then it will be processed by the server, otherwise it will be kept in waiting state.
- **Web_services ():** This process sends the results to *"Check_final_response* ()*"* process.
- **Check_final_response ():** This process validates the response, removes the processed request from the *"valid_request"* table, and sends the result message to the *client* site.

We have improved the proposed mechanism introduced in [25] to get optimal experimental results and feedbacks for protecting cloud-computing systems against application layer based attacks. The performance of the proposed approach is evaluated in terms of *accuracy*, *sensitivity* and *specificity* rates, which computed as following:

$$SYS_{accur} = (T_p + T_n) / (T_p + T_n + F_p + \boldsymbol{F}_n) \times 100\% \quad (1)$$

$$SYS_{sens} = (T_p) / (T_p + F_n) \times 100\% \quad (2)$$

$$SYS_{spec} = (T_n) / (T_n + F_p) \times 100\% \quad (3)$$

Where:
T_p is the No. of cases correctly specified as attacked packets in this experiment.
T_n is the No. of cases correctly specified as normal packets.
F_p is the No. of cases incorrectly specified as attacked packets
F_n is the No. of cases incorrectly specified as normal packets.

In Table 1, we have used various experimental data sizes and thresholds to get the experimental result of the proposed approach. The system is evaluated under both single source and multiple source attack environments in terms of accuracy, sensitivity and specificity.

Table 2. New performance evaluation results

a. DoS Attacks

N	K	T_p	T_n	F_p	F_n	Accuracy	Sensitivity	Specificity
1000	100	40	960	4	2	99.40%	95.24%	99.59%
2000	150	80	1920	8	4	99.40%	95.24%	99.59%
3000	200	120	2880	12	6	99.40%	95.24%	99.59%
4000	250	160	3840	16	8	99.40%	95.24%	99.59%
5000	300	200	4800	20	10	99.40%	95.24%	99.59%
6000	350	240	5760	24	12	99.40%	95.24%	99.59%
7000	500	280	6720	28	14	99.40%	95.24%	99.59%
8000	550	320	7680	32	16	99.40%	95.24%	99.59%
9000	600	360	8640	36	18	99.40%	95.24%	99.59%
10000	700	400	9600	40	20	96.80%	95.24%	99.59%
						99.14%	**95.24%**	**99.59%**
Performance Average								

b. DDoS Attacks

N	K	T_p	T_n	F_p	F_n	Accuracy	Sensitivity	Specificity
1000	100	50	950	5	2	99.30%	96.15%	99.48%
2000	150	100	1900	10	5	99.26%	95.24%	99.48%
3000	200	150	2850	15	7	99.27%	95.54%	99.48%
4000	250	200	3800	20	10	99.26%	95.24%	99.48%
5000	300	250	4750	25	12	99.27%	95.42%	99.48%
6000	350	300	5700	30	15	99.26%	95.24%	99.48%
7000	500	350	6650	35	17	99.26%	95.37%	99.48%
8000	550	400	7600	40	20	99.26%	95.24%	99.48%
9000	600	450	8550	45	22	99.26%	95.34%	99.48%
10000	700	500	9500	50	25	96.40%	95.24%	99.48%
						98.98%	**95.40%**	**99.48%**
Performance Average								

4.1 Performance evaluation of Dos attacks

Ten data sizes (N) of 1000, 2000, 10000 packets were randomly selected, and ten thresholds (K) requests (where $K <= T_p$). The updated version of the algorithm mentioned in [25], was applied and tested to the data according to the window size N, and

the threshold *K*. **In addition to** T_p, T_n, F_p, and $\mathbf{F}_n$, we have two features fed for the implementation of algorithm; these two features are the source IP add and the destination IP add. Table 2-a, presents the experimental results for protect cloud systems against XML and HTTP based DoS attacks. From Table 2-a, we can conclude that the system has *higher performance average* of (97.99%) than the result mentioned in [25], where it has the average percentage of accuracy (99.14%), the average percentage of sensitivity (92.24%), and the average percentage of specificity (99.59%).

4.2 Performance evaluation of DDos attacks

The same data sizes and thresholds stated above are used through the proposed approach to evaluate the performance under DDoS attacks. The experimental results are shown in Table1-b, we can conclude that the system has also a *higher performance average* of (97.95%) than the result mentioned in [25], where it has the average percentage of accuracy (98.98%), the average percentage of sensitivity (95. 40%), and the average percentage of specificity (99.48%).

4.3 Correlation analysis for effectiveness validation

Correlation coefficient is used to identify and analyze the linear relationship between malicious and legitimate traffic. So detecting and identifying the changes of correlation may specify the occurrence of the change. In this section we have presented the effectiveness of the proposed approach, and its efficiency is determined by the suitable data size we could gather in a limited observation window. The proposed statistical model are described by the proposed algorithm below:

Assume in the time interval T_l, n packets are checked. For each feature we obtain n values.

4.4 Proposed correlation algorithm

Inputs: F- Sample of network traffics,

$$f_i^{\,l} = (f_i^{\,l,1}, f_i^{\,l,2}, ..., f_i^{\,l,n}), \text{ and } \quad f_j^{\,l} = (f_j^{\,l,1}, f_j^{\,l,2}, ..., f_j^{\,l,n}) \tag{4}$$

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

$$\text{For each sample } f_i^{\,l} \text{ and } f_j^{\,l} \tag{5}$$

$$\text{Compute: } f_i^{\,l'} = \frac{\sum (f_i^{\,l})}{n} \text{ and } f_j^{\,l'} = \frac{\sum (f_j^{\,l})}{n} \tag{6}$$

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

$$D^{2}(f_i^{l}) = \frac{\sum (f_i^{l} - f_i^{l'})^{2}}{n-1} \text{ and, } D^{2}(f_j^{l}) = \frac{\sum (f_j^{l} - f_j^{l'})^{2}}{n-1} \tag{7}$$

Compute: the covariance of f_i^{l} and f_j^{l} as. $\text{cov}(f_i^{l}, f_j^{l})$ where

$$\text{cov}(f_i^{l}, f_j^{l}) = \frac{\sum (f_i^{l} - f_i^{l'})(f_j^{l} - f_j^{l'})}{n-1} \tag{8}$$

Compute: the correlation coefficient of f_i^{l} and f_j^{l} as: $r(f_i^{l}, f_j^{l})$ where

$$r(f_i^{l}, f_j^{l}) = \frac{\text{cov}(f_i^{l}, f_j^{l})}{\sqrt{D^{2}(f_i^{l}) \times D^{2}(f_j^{l})}} \tag{9}$$

if $r(f_i^{l}, f_j^{l}) \geq \delta$ then "alarm for attack"; Insert_into_blacklist_IP();

else

```
Insert_into_valid_request_table();
Process.client.request();
Get_next_ packets();
```

We note that:

The correlation coefficient of the experimental sample, $r(f_i^{l}, f_j^{l}) \in$ [-1, 1] and evaluates the direction and strength of the linear relationship between f_i^{l} and f_j^{l}.

The correlation between f_i^{l} and f_j^{l} can be positive (*i.e.,* higher levels of f_i^{l} are associated with higher levels f_j^{l}) or negative (*i.e.,* higher levels of f_i^{l} are associated with lower levels of f_j^{l}).

The *sign* of the correlation coefficient indicates the *direction* of the association.

The *magnitude* of the correlation coefficient indicates the *strength* of the association.

If $r = 0$, then there is no linear relationship between f_i^{l} and f_j^{l}.

4.5 Complexity analysis of algorithm

The first step of the proposed algorithm above selects features from given (*F*) samples of network traffics. The complexity of feature extraction is O (*n* x *p*), where *n* is the total No. of packets, in time interval *T,* and *p* is the dimension of each packet. The computation of correlation among multiple features of the instances (packets) needs O

(p x p) time. Therefore, the method takes O (n x m) times to compute Mahalanobis distance (MD) among n instances, where m is the number of elements in an instance. Then the total complexity of the algorithm is O (n x p) + O (p x p) + O (n x m), and since $n \geq p$, and n ≥ m, hence the complexity is O (n).

5 Conclusion

The main objective of this research study is to introduce an effective approach to protect cloud-computing applications against application layer based attacks. Complexity analysis, efficiency and performance evaluations of the proposed approach are introduced. The feedbacks of the experimental results were highly promising, for protecting cloud-computing systems against both DoS and DDoS attacks. Correlation analysis model and algorithm are used to validate the effectiveness of the proposed approach. For Dos attacks detection, we have concluded that the system has higher performance average of (97.99%), where it has the average percentage of accuracy (99.14%), the average percentage of sensitivity (92.24%), and the average percentage of specificity (99.59%). For Dos attacks detection, we have concluded that the system has a *higher performance average* of (97.95%), where it has the average percentage of accuracy (98.98%), the average percentage of sensitivity (95. 40%), and the average percentage of specificity (99.48%).

6 References

[1] Hosam F. El-Sofany, Abdulelah Al Tayeb, Khalid Alghatani, and Samir A. El-Seoud, "*The Impact of Cloud Computing Technologies in E-learning*", *International Journal of Emerging Technologies in Learning* – iJET, Volume 8, Special Issue 1: ICL2012, Pages 37-43, http://dx.doi.org/:10.3991/ijet.v8iS1.2344, January 2013

[2] Final Version of NIST Cloud Computing Definition Published. Available online: http://www.nist.gov/itl/csd/ cloud-102511.cfm (accessed on 14 December t 2017).

[3] Jain, P.; Rane, D.; Patidar, S. A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment. In Proceedings of the 2011 World Congress on Information and Communication Technologies (WICT), Mumbai, India, 11–14 December 2011; pp. 456–461. https://doi.org/10.1109/WICT.2011.6141288

[4] Gowrigolla, B.; Sivaji, S.; Masillamani, M.R. Design and auditing of cloud computing security. In Proceedings of the 2010 5th International Conference on Information and Automation for Sustainability (ICIAFs), Colombo, Sri Lanka, 17–19 December 2010; pp. 292–297. https://doi.org/10.1109/ICIAFS.2010.5715676

[5] McKendrick J., (2011), "Loud Divide: Senior Executives Want Cloud, Security and IT Managers are Nervous", [Accessed 15-12-2017]:http://www.zdnet.com/ blog/ serviceoriented/cloud-divide-senior-executives-want-cloud-security-and-it-managers-are-nervous/6484

[6] Priyanka Chouhan, Rajendra Singh. "Security Attacks on Cloud Computing With Possible Solution", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 1, ISSN: 2277 128X. January 2016.

[7] The information week website.http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085
[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, May 2013.
[9] Rashmi V. Deshmukh, and Kailas K. Devadkar, "Understanding DDoS Attack & Its Effect In Cloud Environment". Procedia Computer Science 49 (2015) 202 – 210. The 4th International Conference on Advances in Computing, Communication and Control" (ICAC3'15), doi: 0.1016/j.procs.2015.04.245.
[10] The Notorious Nine, Cloud Computing Top Threats in 2013, https://downloads.cloud securityallance.org/initiatives/topthreats/TheNotoriousNineCloudComputingTopThreatsin2013 .pdf
[11] Reza M. Sarhadi, and Vahid Ghafori, "New Approach to Mitigate XML-DOS and HTTP-DOS Attacks for Cloud Computing. *International Journal of Computer Applications* (0975 – 8887) Volume 72– No.16, June 2013.
[12] CERT Advisory CA-1998-01, Smurf IP Denial-of-Service Attacks, January 5, 1998, Available: http://www.cert.org/advisories/CA-1998-01.html
[13] Ashley Chonka, YangXiang, Wanlei Zhou, Alessio Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks". Journal of Network and Computer Applications. doi:10.1016/ j.jnca.2010.06.004, Appl 2010.
[14] Srinivas Padmanabhuni, Vineet Singh, K M Senthil Kumar, Abhishek Chatterjee, "Preventing Service Oriented Denial of Service (PreSODoS): A Proposed Approach". IEEE International Conference on Web Services (ICWS'06). 2006 https://doi.org/10.1109/ICWS.2006.102
[15] Adrien Bonguet, and Martine Bellaiche, "*A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing*". Future Internet Journal -. 9, 43, August 2017. https://doi.org/10.3390/fi9030043
[16] Masdari, M.; Jalali, M. A survey and taxonomy of DoS attacks in cloud computing. Secur. Commun. Netw. 2016, 9, 3724–3751; SCN-15-0746.R1.
[17] Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. J. Netw. Comput. Appl. 2016, 67, 147–165. https://doi.org/10.1016/j.jnca.2016.01.001
[18] Denial-of-service attack, Wikipedia, http://en.wikipedia.org/wiki/Denial-of-service_attack
[19] Karnwal, T.; Sivakumar, T.; Aghila, G. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In Proceedings of the 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 1–2 March 2012; pp. 1–5. https://doi.org/10.1109/SCEECS.2012.6184829
[20] Vidhya.V. "A Review of DOS Attacks in Cloud Computing". Journal of Computer Engineering (IOSR-JCE). e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. II, PP 32-35, Sep – Oct. 2014
[21] 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.
[22] B. Prabadevi, N.Jeyanthi, Distributed Denial of service Attacks and its effects on Cloud Environm ent- a Survey, IEEE Explore, 2014
[23] K.Shanti, 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, May 2013.

[24] Amit Vinayakrao Angaitkar, Narendra Shekokar, Mahesh Maurya, The Countering the XDoS Attack for Securing the Web Services, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , pp.3907 -3911,2014.

[25] Hosam F. El-Sofany,"Proposed a Novel Mechanism to Detect and Prevent XML and HTTP-based Denial-of-Service Attacks for Cloud Computing".The 2018 International Conference on Network Technology (ICNT 2018), and 7th International Conference on Software and Information Engineering (ICSIE 2018). Cairo, Egypt on May 4-6, 2018.

7 Authors

Hosam F. El-Sofany received his Ph.D. and M.Sc. degrees in Computer Science. He is currently an *Associate Professor of CS* at King Khalid University, KSA (and Cairo Higher Institute for Engineering, Computer Science and Management, Egypt). He has a strong technical and theoretical background including the development of Web-based and Mobile-based educational systems. His research interest include Cloud computing, E-learning, M-learning, E-health and M-health care applications, fuzzy logic applications, Cloud security, Databases systems, and Semantic web.

Dr. El-Sofany's E-mail: helsofany@kku.edu.sa

Samir A. El-Seoud was born at Alexandria, Egypt, 1944. He received his B.Sc. degree in Physics, Electronics and Mathematics from Cairo University in 1967, his Higher Diploma in Computing from the Technical University of Darmstadt (TUD) - Germany in 1975 and his Doctor of Science from the same University (TUD) in 1979. His research interest is focused among others on: Parallel Numerical Algorithms, Scientific Computations, and Numerical Techniques for Solving Nonlinear Problems, Collaborative Learning, Computer Aided Learning, and Mobile Applications. He held different academic positions at TUD Germany. He has been a Full-Professor since 1987. Outside Germany, he spent several years as a Full-Professor of Computer Science at SQU – Oman, Qatar University, and PSUT-Jordan and acted as a Head of Computer Science for many years. With industrial institutions, he worked as Scientific Advisor and Consultant for the GTZ in Germany and was responsible for establishing a postgraduate program leading to M.Sc. degree in Computations at Colombo University, Sri-Lanka (2001 – 2003). He also worked as an Application Consultant at Automatic Data Processing Inc., Division Network Services in Frankfurt/Germany (1979 – 1980). Currently, Professor El-Seoud is with the Faculty of Informatics and Computer Science of the British University in Egypt (BUE). He published over 90 research papers in conference proceedings and reputable international journals. (E-mail: samir.elseoud@bue.edu.eg

Article submitted 28 November 2018. Resubmitted 29 December 2018. Final acceptance 20 January 2019. Final version published as submitted by the authors.