A Case Study of the Impact of Denial of Service Attacks in Cloud Applications

Hosam F. El-Sofany[1,2], Samir A. El-Seoud[3], and Islam A. T. F. Taj-Eddin[4]
[1]King Khalid University, Abha, Kingdom of Saudi Arabia
[2]Cairo Higher Institute for Engineering, Computer Science and Management, Cairo, Egypt
[3]Faculty of Informatics and Computer Science, British University in Egypt-BUE, Cairo, Egypt
[4]Faculty of Computer and Information, Assiut University, Assiut, Egypt
Email: helsofany@kku.edu.sa, Samir.elseoud@bue.edu.eg, itajeddin@aun.edu.eg

Abstract —Pay for the service is the motto of cloud computing. It allows users to use distributed resources in the Internet to do their computations without installing and paying for those resources. Those resources are diverse to provide services that cover software, platform and infrastructure. When developing services, security is critical especially at cloud computing. Among the numerous cloud attacks that can target the cloud computing systems, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks can cause a major problem in cloud security. One of the main objectives of DoS and DDOS is to consume large amount of server resources so that the server cannot provide service to normal users. Attackers usually gain access to large number of computers by exploiting the vulnerabilities to set up attack armies. This paper will present a comprehensive study for DoS attacks, different detecting techniques of DDoS will be analyzed and reviewed against different parameters, and present an experimental study showing the impact of DoS attacks in cloud applications. This research will measure the stability and validity of the questionnaire's content using Cronbach's alpha, and will determine the impact of the related variables on the result using stepwise multiple linear regression analysis and spearman correlation.

Index Terms—Cloud computing, cloud security, cloud attacks, denial of service attacks, stepwise multiple linear regression, distributed denial-of-service attacks, cronbach's alpha, spearman correlation,

I. Introduction

Historically, mainframe was the first IT technology. It followed by client-server, next was web then Service Oriented Architecture (SOA). Finally, the Cloud had been introduced. By using Internet as intermediary medium of communication, cloud computing providers leverage the delivery of their IT resources on a pay as you go basis to their customers [1].

Whereas cloud computing systems using and sharing a large magnitudes of data. So, the attackers have the motivation, in order to steal the information, the attackers have to explore and exploit the vulnerabilities associated with the cloud. One of the nine major threats to the cloud had been identified by the Cloud Security Alliance (CSA) is Denial of Service (DoS) attacks. In DoS attacks, the attacker simply overwhelms the attacked system with service requests such that it cannot respond or being severely delayed to any more requests. That makes the attacked system unavailable to any user. If several compromised distributed machines are used in the attacks that will be Distributed Denial of Service (DDoS) attack. Those compromised distributed machines had been called zombies. A proper intrusion detection system is needed to be deployed in order to face Dos and/or more frequent DDoS [2].

A DoS attack goal is to make the resources of the computer, i.e. network bandwidth, CPU time, user website…etc, unavailable, overload with traffic or severely slow to the users. Cloud users will not be able to access the services. A large number of compromised computers are used to launch DDoS attacks. In order to counter attack, the DDoS attack, a proper mechanism is needed to identify and eliminate it; otherwise resources will be allocated to the DDoS attacker.

In other hand, in DoS attacks, an attacker tries to affect the browser by inject malicious code into it. The infected browser will try to open as many windows such that legitimate user will not be able to access the service. In addition, an attacker tries to overload the targeted cloud system by overwhelming requests for services. As a result, the targeted cloud system stop responding at all to any requests and the resource will be out of service. DDoS attacks have far worst attacks than DoS attacks [3].

DoS attack is launched most of the cases from a single machine. DDoS attack is launched from many machines. These machine normally are not owned by the attackers, they all hijacked by a malware. The result will be a network of that group of machines, i.e. botnet, which will be used by the DDoS attacker in order to launch the attack. As the attack may be distributed over multiple machines, it will be very hard to differentiate authentic users from attackers.

II. DoS and DDoS Review

When developing services on the cloud, security should be critically considered [4]. Some aspects that challenging cloud computing are:

- **Identity**

Manuscript received July 25, 2018; revised January 17, 2019.
doi:10.12720/jcm.14.2.153-158

- **Authentication**
- **Authorization**
- **Confidentiality**[5]
- **Integrity**
- **Isolation** [6-7]
- **Availability**

In a DDoS attack, hosts, i.e. bots or zombies, could be virtual machine, PC or laptops. They have the feature of being controlled remotely. Using a large number of hosts at the attack is A DDoS. DDoS is more disruptive than DoS. A collection, i.e. hundreds of thousands, of bots is known as a "botnet". The DDoS attack generally targets the bandwidth of the communication, resources such as memory buffers, and protocols of network or the logic of the application processing.

A. Dos and DDoS attacks

Authors realized the magnitude and potential of Dos and DDos attacks during their researches at e-learning, m-learning and cloud computing in e-learning process [8-14]. Two objectives DoS and DDoS can have. Overwhelming the resources of the target system is the first. Exploring and exploiting the vulnerabilities exist in the system is the second [15]. See Fig. 1.

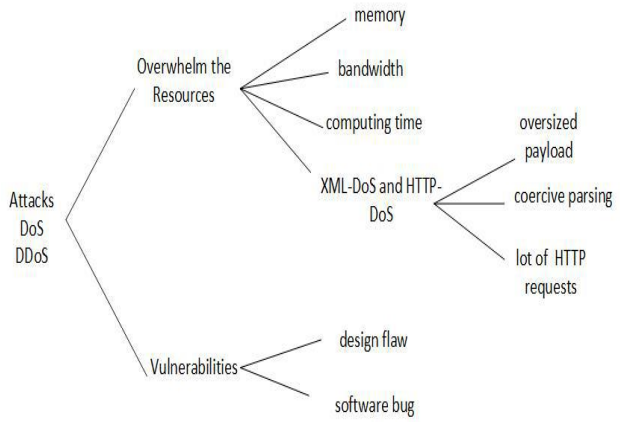

Fig. 1. The two objectives of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks [16].

- **Overwhelm the Resources**
  - **Exhausting Memory:** Internet protocols and networking devices vulnerabilities could be used in the attack, i.e. SYN (SYNchronize) flood attacks. Proxy applications can prevent such attacks.
  - **Exhausting Bandwidth:** The attack exhausts the bandwidth [17].
  - **Exhausting Computing Time/Bandwidth:** That attack is based on stealing time computing and computing bandwidth from other users. A huge amount of external entities that had been referenced at exist at SOAP, i.e. Simple Object Access Protocol, messages will push the server to try to open a huge number of connections, i.e. TCP connections, and a huge amount of cycles, i.e. CPU cycles. That is a huge waste in the process.
  - **XML-DoS and HTTP-DoS:** when it comes to attacks of DoS and DDoS in Cloud Computing, HTTP-DoS and XML-DoS are probably the most destructive attacks [18]. In cloud computing, the web services are depending heavily on HTTP and XML. With XML encryption, the legitimacy of the request is implicitly assumed.
    - Three strategies are used at the case of SOAP uses XML. The first is to use an oversized payload, such that resources of the targeted system will be consumed. The second is to force the server to deal with many huge remote XML files defined within DTD. The third is to force the server to heavily use the CPU and the memory to recursively deal with entities defined within the DTD.
    - XML-DoS attack, i.e. the Coercive Parsing attack, is exhausting the CPU and the memory by using a continuous sequence of deeply nested XML structures, namespace URIs, …etc [19], [20]
    - An HTTP-DoS attack sending a huge amount of HTTP requests. Next a repetition of requests will be made by HTTP that recursively attack a specific web service [19].
- **Exploit the Target System's Vulnerabilities:** Another kind of attack aims at discovering vulnerabilities that can help in the Dos or DDoS attacks. That discovery is happening systematically [15]. The attacks will take advantage of the design flaw, software bug,…etc. A service degeneration or crash will be the result of the attack.

B. DoS and DDoS Defense

In order to stop the attacks of DoS and DDoS, the source of the attack should be identified and blocked. That makes difficult DoS and DDoS attacks defending against. The following is a brief of strategy against DoS and DDoS [16]:

- **Prevention:** An exhaustive and standardized Service level agreement is a necessity. By having a Service level agreement between a client and the service provider, the client will have a legal agreement for availability, confidentiality, trust, protection and security [21].

  Attack Mitigation: In order to eradicate an attack, five requirements are needed [22]. First, detect the attack and its magnitude ASAP. Second, mitigate the effects of the attack. Third, if step two failed, then migrate the attacked virtual machine to safe location. Fourth, maintain network bandwidth. Fifth, face and put an end to the attack.
- **Security Architecture:** Several elements involved at security architecture such as servers, switch controller, protocols, router and applications. At [22] and to

defend against DDoS attacks, a migration of virtual machines had been proposed at federated cloud architecture. At [23] an architecture using Software Defined Networking to DDoS attack mitigation had been proposed. Hybrid Firewalling Architecture had been proposed at [24].

- **XML-DoS and HTTP-DoS Attacks Defenses:** defenses against that type of attacks had been developed, such as, filtering tree [21]. Cloud Trace Back (CTB) [25], [26] and Using CAPTCHA [27].

C. DoS and DDoS Defense System Evaluation

Researches must using metrics and conduct experiments to assess the performance and value of the defenses of DDoS attacks. They could use simulation, testing, implementation of proposed solutions. The following is a brief of DDoS attacks evaluation defense systems [16]:

- **Theoretical Evaluation:** Defense system total time consumption theoretically evaluation [28].
- **Collection of Data:** Sets of data had been used in order to evaluate the proposed system [29].
- **Simulation:** Simulating attacks with changing parameters [30]
- **Testbed:** Using hybrid cloud infrastructure with partial simulation [19], [23], [25], [26], [31], [32].

III. Research Study Hypothesis

The authors focus on testing a key hypothesis in order to handle the dimensions of the research problem and objectives as follows. The research *key hypothesis* is identified as following:

"*There is a negative impact with different dimensions from the Denial of Service attacks in cloud applications in higher education environments".*

IV. Analysis of Research Study

The research variables are divided into:

- *Independent Variables*: Independent Variables: include independent dimensions that affect for the users of cloud computing applications in the learning organization through the problem of "denial of service attacks".
- *Dependent Variable:* the variables that affect the experimental results will be included and translate the feedbacks of the users regarding the proposed problem.

Spearman Correlation was used by the authors to identify and measure the relationship and direction between independent and dependent variables.

On the other hand in order to measure stability and validity of the questionnaire's contents of the study the authors will use cronbach's alpha. The questionnaire is reviewed and verified for its validity and completeness to statistical analysis and data entry. The experimental variables were coded and the statistical computations are done by SPSS (Statistical Package for Social Sciences). The following dependent variables are considered:

- Gender
- Age
- Job
- College
- Department
- City
- Education level

The descriptive statistics, i.e. of the selected dependent and independent variables that related to the research samples, were extracted by the authors. Arithmetic mean, standard deviation, coefficient of standard variation,…etc, are included in the descriptive statistics.

The results in this research paper are based on data from questionnaires of conducted survey by the authors from January 1 to February 25, 2018, among a sample of 1904 adults (799 males and 1105 females).

The following results describe the Likert Scale evaluation for the questionnaire responses towards the given problem:

- 16% of users are "very satisfied",
- 05% of users are "neutral",
- 48% of users are "strongly agree",
- 27% of users are "agree", and
- 04% of users are "disagree",

Cronbach's Alpha had been measured and found to be (0.8446). That means the study samples has a high degree of validity, i.e. that the face validity of the content of the proposed views that had been reflected on the study samples validity has reached (0.8586). The authors determined the characteristics of the study sample using the descriptive statistics referred to above as described at the following sub-section.

A. Demographic Variables Descriptive Statistics

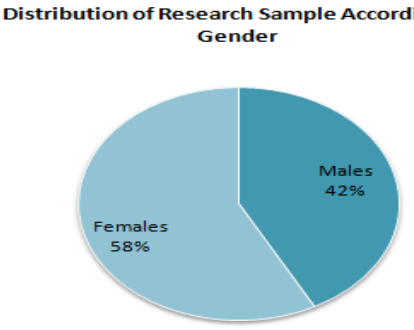

Fig. 2. *"Gender"* based research samples distribution.

The demographic variables descriptive statistics in the research experiments includes: *gender, age, job position, college, department, city, education level.*

- The "*gender*" based research samples distribution is shown in Fig. 2. *Female* sample got 57.8% and *males* sample got 42.2%.
- The *"age"* based research samples distribution is shown in Fig. 3, it categorized into two groups: "*age*"

group from 23 to less than 60 years (staff and employees) was the highest; 75.0% followed by other age group from 18 to 22 years (students) was 25.0% of the research sample individuals.

- On the other hand, the distribution of the research samples according to "*job position*" is categorized into three groups: first is the "*academic staff*" group was the highest; 50.25%, followed by the "employees" group was; 11.25%, and finally the "*students*" group was; 38.5%, as shown in Fig. 4.

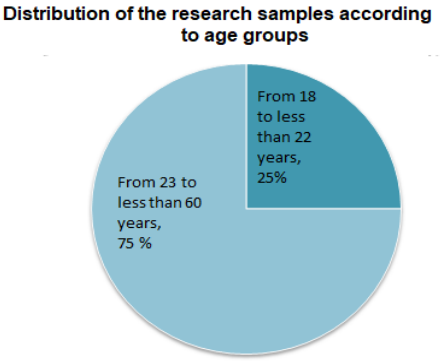

Fig. 3. Distribution of Research Samples according to *age Groups*

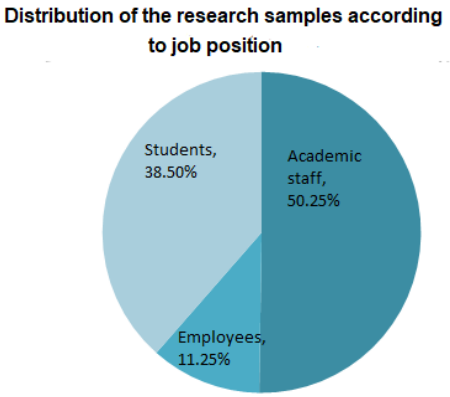

Fig. 4. *"job position"* based research samples distribution

V. Research Results

In this section authors are presented the *independent* variables descriptive statistics explaining table's data related to such variables. Tables are showing the items that obtained highest agreement or lowest agreement or disagreement depending on the research samples responses.

A. The Effect of DoS Attacks the Users

Table I shows the directions of the research samples suggested by the researchers towards "*the effect of DoS Attacks in cloud on the users*". The statistics results of this questionnaire are: (1.984) for arithmetic mean and (53.75%) for coefficient of standard variation. Some of selected *items* include:

I1-Trust is important in the Cloud computing environment

I2-We are highly trusted in the use of cloud based systems

I3-The DoS attacks are destructive and depend on the security staff expertise level of cloud systems.

I4-The DoS attacks are negatively affecting the reliability the usage of cloud base computing systems.

I5-Even if DoS attacks happen; the working capacity of the cloud should be enough to keep services running and offered.

I6-There is a need to use a restricted model to impose strict user's registration standards, these may avoid probably from the denial of service attacks.

I7-Cloud computing future is in danger if not a sufficient measure is in place to overcome DoS attacks and its rapidly increasing damages and frequency.

I8-It is totally disappointing to the user when he/she need an urgent service, which he/she paid for, and he/she does not find it; instead a cold technical error message is all what he/she got.

I9-Authors believe that a serious thinking about authentication procedures and user's information validation are more fruitful in order to avoid aforementioned security attacks.

I10-Two reasons caused the less effectivity of hijacking attacks. The first, done by cloud service provider, is the using of firewalls and anti-malware. The second is the series enforcement of cyber laws in many countries including Egypt and KSA.

B. Spearman Correlation Analysis

The Spearman Correlation is used to identify and measure the relationship and direction between dependent and independent variables. The following results are deduced from Table I.

- There is a positive relationship between independent and dependent variables related to research sample, this means that, there is a negative impact with different dimensions from the DoS attacks in cloud based systems, at a significance level less than (0.02), (0.05) which proves the validity of the research key hypothesis.

Table I: The Descriptive Analysis of "The Effect of DoS Attacks in Cloud on the Users".

Items	Weighted Arithmetic Mean	Standard Deviation	Coefficient Of Standard Variation	Order
I1	1.83	1.021	55.71	5
I2	1.89	0.899	48.75	2
I3	1.98	1.181	53.81	4
I4	1.71	0.971	51.89	3
I5	2.12	1.201	57.98	9
I6	2.15	1.269	56.96	7
I7	2.02	1.140	59.26	10
I8	2.37	1.241	55.74	6
I9	1.93	1.176	57.70	8
I10	1.82	0.603	44.65	1

VI. Conclusions & Future Works

This paper presented a comprehensive study for DoS; different DDoS detecting techniques had been analyzed and reviewed against different parameters. This paper has

introduced an experimental study showing the impact of denial of service attacks in cloud applications. The results of this research study figured out the need of good mechanism to prevent the Denial of Service attacks of cloud applications in higher education environments that affect the performance of academic staff and employee works. The authors conducted a case study at King Khalid University, in Saudi Arabia, and presented an experimental study showing the impact of denial of service attacks in cloud based systems. The research measures the stability and validity of the content of the questionnaire using Cronbach's alpha. Also, the research determines the impact of the related variables on the results using spearman correlation analysis. As a future work, the types of DDoS attacks that face the cloud based academia applications will be identified and the expected solution associated to each problem will be proposed.

REFERENCES

[1] H. F. El-Sofany, A. Al Tayeb, K. Alghatani, and S. A. El-Seoud, "The impact of cloud computing technologies in e-learning," *International Journal of Emerging Technologies in Learning*, vol. 8, no. 1, pp. 37-43, January 2013.

[2] 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

[3] T. Karnwal, T. Sivakumar, and G. Aghila, "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack," in *Proc. IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, India, 1–2 March 2012, pp. 1-5.

[4] T. Sridhar, "Cloud computing: Infrastructure and implementation topics," *Int. Protoc. J. CISCO*, vol. 12, no. 4, 2009.

[5] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," in *Proc. 16th ACM Conference on Computer and Communications Security*, Chicago, IL, USA, 9–13 November 2009; ACM: New York, NY, USA, 2009, pp. 199–212.

[6] K. Hashizume, D. Rosado, E. Fernandez-Medina, and E. Fernandez, "An analysis of security issues for cloud computing," *J. Int. Serv. Appl.*, vol. 4, no. 5, 2013.

[7] N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho, M. Simplicio, G. de Sousa, and M. A. Pourzandi, "Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing," in *Proc. IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom)*, Athens, Greece, 29 November 1 December 2011, pp. 231–238.

[8] H. F. El-Sofany, A. Al Tayeb, K. Alghatani, and S. A. El-Seoud, "The Impact of cloud computing technologies in e-learning," *iJET* , vol., 8, no. 1, Jan. 2013.

[9] M. S. El-Seoud, H. F. El-Sofany, I. A. T. F. Taj-Eddin, A. F. Nosseir, and M. M. El-Khouly, "Implementation of web-based education in Egypt through cloud computing technologies and its effects on higher education," *Studies in Higher Education*, vol. 3, no. 3, pp. 62-76, May 2013.

[10] M. S. A. El-Seoud and I. A. T. F. Taj-Eddin, "Developing an android mobile bluetooth chat messenger as an interactive and collaborative learning aid," in *Intelligent Systems and Computing, Interactive Collaborative Learning*, M. Auer, D. Guralnick, and J. Uhomoibhi, Eds., Springer, Cham., 2016, vol. 545, pp. 3-15.

[11] M. S. A. El-Seoud and I. A. T. F. Taj-Eddin, "Beyond android: An essential integration for better utilization," in *Proc. International Conference on Interactive Mobile Communication Technologies and Learning*, IEEE, pp. 98-102.

[12] M. S. A. El-Seoud, H. F. El-Sofany, and I. A. T. F. Taj-Eddin, "Mobile applications and semantic-web a case study on automated course management," *International Journal of Interactive Mobile Technologies*, vol. 10, no. 3, pp. 42-53.

[13] M. S. A. El-Seoud, M. El-Khouly, and I. A. T. F. Taj-Eddin, "Strategies to enhance learner's motivation in e-learning environment," in *Proc. 18th International Conference on Interactive Collaborative Learning*, 2015, pp. 944-949.

[14] M. S. A. El-Seoud, H. F. El-Sofany, A. Karkar, A. Dandashi, I. A. T. F. Taj-Eddin, and J. M. AL-Ja'am, "Semantic-Web automated course management and evaluation system using mobile applications," in *Proc. 18th International Conference on Interactive Collaborative Learning*, 2015, pp. 271–282.

[15] J. Antunes, J, N. Neves, and P. Verissimo, "Detection and prediction of resource-exhaustion vulnerabilities," in *Proc. 19th International Symposium on Software Reliability Engineering*, Seattle, WA, USA, 10–14 November 2008, pp. 87–96.

[16] A. Bonguet and M. Bellaiche, "A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing," *Future Internet*, vol. 9, no. 43, 2017.

[17] H. Liu, "A new form of DOS attack in a cloud and its avoidance mechanism," in *Proc. ACM Workshop on Cloud Computing Security Workshop*, Chicago, IL, USA, ACM: New York, NY, USA, 2010, pp. 65–76.

[18] X. Ye, "Countering DDoS and XDoS attacks against web services," in *Proc. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Shanghai, China, December 17–20 2008, vol. 1, pp. 346–352.

[19] T. Vissers, T. S. Somasundaram, L. Pieters, K. Govindarajan, and P. Hellinckx, "DDoS defense system for web services in a cloud environment," *Future Generation Computer. Systems*, vol. 37, pp. 37–45, 2014.

[20] S. Padmanabhuni, V. Singh, K. S. Kumar, and A. Chatterjee, "Preventing service oriented denial of service (PreSODoS): A proposed approach," in *Proc. International Conference on Web Services*, Chicago, IL, USA, September 18–22, 2006, pp. 577–584.

[21] B. Kandukuri, V. Paturi, and A. Rakshit, "Cloud security issues," in *Proc. IEEE International Conference on*

Services Computing, Bangalore, India, September 21–25, 2009, pp. 517–520.
[22] J. Latanicki, P. Massonet, S. Naqvi, B. Rochwerger, and M. Villari, "Scalable cloud defenses for detection, analysis and mitigation of DDoS attacks," in *Towards the Future Internet*, IOS Press: Amsterdam, The Netherlands, 2010, pp. 127–137.
[23] B. Wang, Y. Zheng, W. Lou, and Y. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," in *Proc. IEEE 22nd International Conference on Network Protocols (ICNP)*, Raleigh, NC, USA, 21–24 October 2014, pp. 624–629.
[24] F. Guenane, M. Nogueira, and G. Pujolle, "Reducing DDoS attacks impact using a hybrid cloud-based firewalling architecture," in *Proc. Global Information Infrastructure and Networking Symposium (GIIS)*, Montreal, QC, Canada, September 15–19, 2014, pp. 1–6.
[25] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," *J. Netw. Comput. Appl. Elsevier*, vol. 34, pp. 1097–1107, 2011.
[26] A. Chonka and J. Abawajy, "Detecting and mitigating HX-DoS attacks against cloud web services," in *Proc. 15th International Conference on Network-Based Information Systems (NBiS)*, Melbourne, Australia, September 26–28, 2012, pp. 429–434.
[27] A. S. Sairam, S. Roy, and S. K. Dwivedi, "Using CAPTCHA selectively to mitigate HTTP-Based attacks," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, December 6–10, 2015, pp. 1–6.
[28] S. Zhao, K. Chen, and W. Zheng, "Defend Against Denial of Service Attack with VMM," in *Proc. Eighth International Conference on Grid and Cooperative Computing*, Lanzhou, China, August 27–29, 2009, pp. 91–96.
[29] K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection for grid and cloud computing," *IT Prof.*, vol. 12, pp. 38–43, 2010.
[30] M. Liu, W. Dou, S. Yu, and Z. Zhang, "A clusterized firewall framework for cloud computing," in *Proc. IEEE International Conference on Communications (ICC)*, Sydney, Australia, June 10–14, 2014, pp. 3788–3793.
[31] M. A. Saleh and A. A. Manaf, "A novel protective framework for defeating HTTP-Based denial of service and distributed denial of service attacks," *Sci. World J.*, p. 19.
[32] T. Halabi and M. Bellaiche, "How to evaluate the defense against DoS and DDoS attacks in cloud computing: A survey and taxonomy," *Int. J. Comput. Sci. Inf. Secur*., vol. 14, pp. 1-10, 2016.

Hosam F. El-Sofany received his Ph.D. and his 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 background including the development of Web-based and Mobile-based educational systems. His research interest include: Cloud computing, Cloud security, E-learning, M-learning, Databases systems, and Semantic web. 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, 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

Islam A. T. F. Taj-Eddin received his Ph.D., M.Phil. M. S. all in Computer Science from the City University of New York in Fall 2007, Spring 2007 and Spring 2000 respectively. His BSc degree in Computer Science, from King Saud University in Spring 1997. Dr. Taj-Eddin held different academic positions at USA and Egypt. He was an Adjunct Assistant Lecturer at Lehman College of the City University of New York, and Fordham College at Rose Hill of Fordham University. He was a Lecturer at Alexandria Higher Institute of Engineering & Technology at Alexandria city of Egypt. Later he became a Lecturer at the British University in Egypt. He has published almost a dozen refereed research papers related to Algorithms, E-learning, Web-Based Education, Software Engineering, Technology for special needs users and Information Technology. He is interested also in the subject of quality assurance in research and education. Currently he is a Lecturer at the IT dept., FCI, Assiut Univ. E-mail: itajeddin@aun.edu.eg; islam_t@hotmail.com.