A Novel Model for Securing Mobile-based Systems against DDoS Attacks in Cloud Computing Environment

https://doi.org/10.3991/ijim.v13i01.9900

Hosam F. El-Sofany(✉)
King Khalid University, Abha, Kingdom of Saudi Arabia
Cairo Higher Institute for Engineering, Computer Science and Management, Cairo, Egypt
helsofany@kku.edu.sa

Samir A. El-Seoud
British University in Egypt, Cairo, Egypt

Abstract—The increasing growth of mobile devices technology and Mobile-based systems with the emerging of cloud computing technology, created a Mobile Cloud Computing field to be the recent future technology for different wireless services. The development of Mobile-based system under cloud computing environment solve some performance and environment related issues include: bandwidth, storage capacity, availability, scalability and heterogeneity. The Mobile-based cloud computing apps are different comparing to mobile computing apps, since in the first model the devices run cloud based web applications not as mobile computing native apps. Services of Mobile-based systems via cloud are accessing and sharing through internet connection thus they are open for attacker to attack on its security. Distributed Denial of Service (DDoS) attacks can cause a big problem in mobile cloud computing security. The main objective of DDoS attacks is to infect wireless devises resources (e.g., software applications, wireless network, etc.) and make them unavailable to the authorized user. In DDoS, the attacker tries to overload the Mobile-based service with traffic. The main objective of this research paper is to introduce novel model for securing Mobile-based systems against DDoS attacks. Efficiency and performance analysis evaluations of the proposed model are presented. The feedbacks of the experimental results were highly promising, for protecting mobile-based cloud computing systems against DDoS attacks.

Keywords—Mobile computing, cloud computing, mobile security, mobile attacks, denial of service attacks, distributed denial-of-service attacks

1 Introduction

The use of mobile have become an essential part of human life. The growing need for mobile and wireless devices is a positive sign that these devices are playing an important role in human life also. Mobile devices specially are being used for text, voice, and video chat (via social apps) as well as for information exchange. Since most of individual have a mobile device, so the development of Mobile-based apps provides

them with fast access to information they needed in their lives. Therefore, mobile devices have become instruments that allow new ways of interacting with institutional services [1].

The rapid development of mobile technology and mobile computing fields became a strong effect in the development of both wireless communications technology (hardware) and mobile-based apps (software). Mobile cloud computing is the development and implementation of mobile computing apps under the cloud computing models. This will provide full access to all Mobile-based cloud services through the cloud anytime, and from anywhere. Therefore, mobile cloud computing is becoming a future technology, and the solution of its security issues become in focus for scientific research studies [2].

Using mobile devices to access and run software apps have some related limitations include: limited computing ability, processing power, and limited storage capacity. To avoid these limitations, the idea of *cloud computing* is introduced as the use of external computing resources that provides the services over Internet [3].

Attacks to the mobile devices and apps security have been increasing significantly. Attackers may use various attack ways, such as cutting data access that among mobile devices and putting infected code into mobile apps to gain access to users' private information. These attacks are done by easy way via by weakness in the mobile design, and the ways of using the mobile. Some weakness include: a failure in the authentication of user username or password, and the operating system is not updated by recent versions continuslly [4].

Many research studies have been done in the *network security* and *cloud security* fields but security of mobile computing in cloud computing environment is something new and challengeable. In direction of cloud computing security many valuable research studies were published. Recently, mobile cloud computing security is having some problems according to vulnerabilities in mobile devices and the existence of new mobile attacks [5].

Mobile computing security needs to provide some important objectives for data communication include: availability, authentication, accountability, confidentiality, integrity, and portability. Therefore, the need to provide un-cutting session when user wants to move from one URL link to another without any intervention has created motivation for the attackers to perform many attacks on the mobile devices [6].

Our research study focuses on understanding and modeling Denial of Service attack that represents one of dangerous and destructive attacks for mobile computing devices and apps. 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 a large number of machines to launch the DDoS attacks, to overload the wireless network and mobile CPU. This will be in the absence of any good mechanisms to face DDoS attacks DDoS attacks are frequently increasing and target mobile computing systems. This issue opened many research areas and motivated the authors to study the problem and to innovate a proper approach to protect mobile-based systems against this type of attacks [16].

The paper is consists of seven sections as follows: in section two, we present some related and previous research work done in the same topic. In section three, we present

a brief introduction about cloud computing' architecture, model, characteristics, deployment, and security. In section four we present attacks categories on mobile devices and its apps. In section five we discuss Denial of Service attacks issue for mobile device and its apps, and present the main goal of the DDoS attacks for mobile-based systems running in cloud environment. In section six we introduce the proposed model and its performance analysis evaluations for securing mobile-based systems against DDoS attacks in cloud computing environment. The paper finally concluded in section seven.

2 Related Work

In [8] the authors presented security technique on mobile phones, by defining some critical weakness of existing models of security. The authors have shown how such weakness can be used to publish DDoS attacks to public service infrastructures by redirect phone calls. This is done by infecting a specified code through the process of overflow. The authors also demonstrated that, by only use1% of Linux-based mobile apps, the service of an emergency-call center in a region with millions of population can be disabled or denied [7].

In [9] the researchers discussed several weakness points of the UMTS security architecture that can be used by bad attackers to publish DoS attacks. They have shown that an attacker tries to access unsecure control messages in order to manipulate specific actions. They have presented many examples of these such attacks includes:

- **Dropping ACK signal:** In this case the attacker monitors the Temporary Mobile Subscriber Identity allocation command messages and then leave any following TMSI allocation complete message to repeatedly forced the creation of new one, as a result will cause a denial of service attack to all the users in that location.
- **Modification of unprotected RRC messages:** In this case the attacker replaces a valid RRC (Radio Resource Control) connection message with a reject RRC connection, as a result the quality of service (QoS) will be low, and this will lead at the end to DoS attack.
- **Modification of the initial security capabilities of mobile station (MS):** In this case attacker updates the RRC connection request message and this will lead to the termination or failure of connection. This type of attack can do a dangerous damage by implementing a very large number of connection requests simultaneously.
- **Modification of authentication messages:** This case will done if the Radio Network Controller (RNC), on getting a required message, releases the connection, and disconnecting the MS.
- **SQN synchronization:** In SQN (Sequence Number) case, an attacker can require a resynchronization procedure to be running simultaneously for a large number of users, and repeatedly, this will cause greatly overstress the Home Location Register (HLR) of the user's home network (HN).
- **Extensible Authentication Protocol and Authentication Key Agreement Protocol - EAP-AKA:** In this case the attacker can fraud an EAP-Response/AKA-client message and send it to the EAP server to force it into stopping the protocol or can

fraud an EAP-Response/AKA synchronization by failure notification to force the server to make the costly resynchronization procedure [7].

In [10] the authors presented an attack where a bad user imitates a valid Global System for Mobile communications (GSM) base station to a Universal Mobile Telecommunications System (UMTS) subscriber and, as a result, the attacker can spy on all mobile calls and apps [7].

In [11] the authors investigated the chance of a DoS attack by useful advantage of a specific flow found in the UMTS security model. This attack include the update of the RRC connection Request Message that includes the user's device security capabilities. This message is not full protected and in case of mismatching, the connection will be terminated, but during this process enough resources will be consumed at both sides [7].

The researcher in [12], presented and discussed the types of failure that can be resulted to mobile phones, such as: violation of privacy, theft the identity and emergency call number and distribution of DoS attacks [7].

In [14] the authors proposed cross-layer model for quality of service (QoS) signaling protocol in Mobile Ad Hoc Networks (MANETs), which provides protection against class of DoS attacks. The presented model uses distributed rate control to control the bandwidth resources of the network, but does not depend on the maintenance of per-flow state. In this model, each mobile node preserve a state table bandwidth limit reservations, which grow as a function of the number of neighbor nodes rather than the number of traffic flows traversing the node. The proposed protocol provides quality of service signaling on top of an arbitrary MANET routing protocol and uses mechanisms at the Media Access Control layer (MAC) for QoS provisioning and resistance to attacks in conjunction with the signaling protocol. The key media access control layer elements of the scheme consist of evaluating the available wireless range, traffic policing, and rate controlling, all of which are performed in a distributed way in the network. But this solution prone to state table exhaustion [13].

The researchers in [15] proposed a process model to characterize the evolution of node behaviors and studied the problem of node isolation where the effects of DoS attacks are done. The proposed model is used to describe the evolution of node behaviors, and the randomly property of the model is analyzed to show the effects of node behaviors. The node isolation problem is tested by examining the cooperative degree, and the probabilistic connectivity of specific nodes is obtained by using the randomly property of node behaviors. The survivability of wireless ad hoc net-works is analyzed probabilistically, and its theoretical bounds are derived in closed forms, which is used to evaluate the impacts of different behaviors [13].

In this research study we extend the proposed mechanism introduced in [16] to protect Mobile-based cloud systems against DDoS.

3 Cloud Computing Model

Cloud computing architecture consists of three service layers called: Software as a Service (SaaS); Platform as a service (PaaS) and Infrastructure as a service (IaaS).

Therefore, Cloud computing model is introduced as five components that comprise: *clients*, *applications*, *platforms*, i*nfrastructure* and *servers*. Cloud model promotes availability and is consist of five essential characteristics that provide (1) high scalability and elasticity, (2) availability and reliability, (3) performance and optimization, (4) accessibility and portability, and (5) manageability and interoperability [17].

The present clouds are published in one of four deployment models: (1) Private cloud: the cloud infrastructure is provided for private used by a single organization comprising of multiple users. (2) Community cloud- in which the cloud infrastructure is provided for specific use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations), (3) Public cloud- in which the cloud infrastructure is provided for open use by the general public, and (4) Hybrid cloud - in which the cloud infrastructure is consists of two or more cloud infrastructures [17].

Cloud computing Security is critical when developing cloud applications and services. Cloud security concerns arise because the customer data, information, and programs are stored in the servers of cloud provider. Cloud computing security identifies some important objectives include: *Availability, Authentication, Accountability, Confidentiality, Integrity, and Portability* [16].

The above security objectives require; use of certain *security mechanisms* and *services* to be developed, for improving cloud computing security. A s*ecurity mechanism* can be defined as a process which aimed to detect or/and prevent a security attacks. 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.

4 Attacks on Mobile Devices and Mobile Apps

The research studies show that attackers are now focusing increasingly on mobile apps and devices. Mobile and wireless devices use many apps through the internet and www connection that cases them a main goal for attackers that motivated destroy and prevent security mechanisms and cause apps failure and threats. This situation requires increasing efforts against attackers to avoid or minimize the bad effects that infect mobile device and apps. This will done by innovate mobile device security mechanism and propose solutions for security issues continual [18]. Attackers are infect the weak point in the mobile connection and enhancing the most successful scams for infecting the mobile apps.

The types of mobile attacks are divided into four categories include [19]:

Physical Based Attacks: Mobile and wireless devices are manufacturing for using them in daily life. So, the security of the mobile machine is an important field. Some of mobile physical attacks are presented: [20, 21, 22]:

- *Bluetooth*: It supports the short-range radio technology for exchanging data over short distances. So many active attacks, and vulnerabilities can effected mobiles

through Bluetooth. Also malware can transfer from mobile to mobile through Bluetooth services.
- *Lost or stolen mobiles*: The loss and theft of mobile devices are form a dangerous threat since these software apps and hardware devices can be resold on the market, which threatens a user's personal private and sensitive information

Application Based Attacks: Many download apps and files are free over the internet, and most of them have serious security issues. Also, free malicious software and apps are available on different web pages and websites, contain great fraud and scams. Application based attacks can be classified as following [20, 21, 22]:

- *Denial of service attack*: In this type of attack, the attacker denies the access of app services to the mobile users. With mobile hardware problems, an experienced attackers can infect mobile device with a small effort, and even one or two attackers may be enough to infect mobile and make it unsafe.
- *Spyware*: This programs is developed to gather personal and private information without a user's acceptance. It focuses on data and typically include the user's location, contact list, private photos, financial information, emails, history of user browser, and user call history.
- *Malware*: Is a malicious program executes malicious actions after installed itself in a user's mobile without taking user acceptance. It can add charges to any invoice of a user, send junked messages to user's contact list, and give an attacker the authority to access the mobile device.
- *Vulnerable application*: Applications that contain faults and used with malicious intent to infect mobile devices and apps. It gives the attackers the authority and permission to perform unwanted process such as: access private, personal, business information, and download apps without approval.
- *Privacy attacks*: It can be caused by mobile apps and malicious apps. For example, the GPS can provide information about places visited by a user. The attacker can steal this information which may cause dangerous problems.

Network Based Attacks: Mobile and wireless devices provide good support to cellular networks and wireless LAN, both network models may have different types of attacks, some of them include [20, 21, 22]:

- *Network exploits*: This attack uses the weakness of the mobile OS or other apps that operates on the wireless networks. When the mobiles are connected through a wireless network, attackers install some bad and malicious programs on users' mobile without their acceptance.
- *Mobile network services*: Mobile services such as SMS, MMS, and voice calls can be used for attacking mobile devices. By this way, a new attack called "phishing" attack will infect mobile devices. A phishing attack collects sensitive and private information from the user by representing itself as an authorized user or device.
- *Wi-Fi sniffing*: This involves the interruption of data among mobiles and the Wi-Fi access point from the air. It considers that every mobile apps and web pages has

some weakness. Thus, passing data in the Wi-Fi medium is a big risk. Unencrypted data can easily be collected by attackers.

Cloud-Based Attacks: The users of mobile always use cloud-based apps over the wireless internet. Thus attacks related to such process is a major concern, and many researches proved that cloud-based attacks are very serious problem for mobile devices some of them include:

- *Drive by downloads*: This include automatic download of mobile apps from malicious web page addresses.
- *Browser exploits*: This type of attack u the weakness points of Web browser or an app used the browser of the user's mobile. Generally, when user visiting an unsafe website, clicking in a browser can install and run an infected program or apps on a victim mobile device, where the attacker has full control and can expose the user's date and facilitate data privacy theft.
- *Phishing scams*: It is a way of attacker to steal user's private and business information by using them as a reliable users using a link on a social networking website, chat, spam email, or malicious website.

5 Denial of Service Attacks for Mobile Device and Apps

The main goal of the DDoS attack is to deny services accessibility of a mobile app or a mobile device itself. The facing of mobiles DDoS attacks are mostly due to strong connectivity and reduced capabilities which includes: the limitation of mobile hardware power, attacking a mobile can be done with a small effort of attacker. DDoS attack could quickly uses the mobile batteries, shutdown or limit the operation time and CPU perform, these tasks require a lot of energy or force to shut down the mobile. Another type of DDoS that sends a very large amount of SMS or MMS to the same mobile number to either deny users to achieve their objectives or infect the apps services [7]. Since using SMS communications for sending messages between mobile devices, low-end mobile can be forced to shut down. For this purpose, the SMS protocol can be used to transfer small bad programs that can execute on a mobile. Network operators use these files to change the settings on a mobile device [23].

For mobile-based systems running under cloud computing environment, the main objective of the DoS and DDoS attacks is to target and infect cloud resources. Dos attack causes serious damages for cloud services, so it is essential to develop a detection mechanism for protecting mobile-based apps that using cloud computing services [5].

The DOS attack is usually published from a single machine, as opposed to a DDOS attack which is published from multiple machines. Naturally these machines aren't all owned by the attacker. These machines are usually added to the hacker's network by means of *malware.* This group of machines is called a *botnet*. As the attack may be distributed over multiple machines, it will be very hard to differentiate authorized users from attackers. In DoS attacks, the attacker tries to overload the target Mobile-based system with web service requests so that it cannot respond 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 (called master) uses several compromised machines called *zombies* to launch DoS attack on the target device (victim), and as a result service will be delayed or/and stopped, as shown in Figure (1). 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 as a result deny authorized users access to cloud services. In addition, an attacker tries to overload the target cloud based system through mobile with service requests in order to stop responding to any new requests and hence made resources unavailable to its 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 [5].

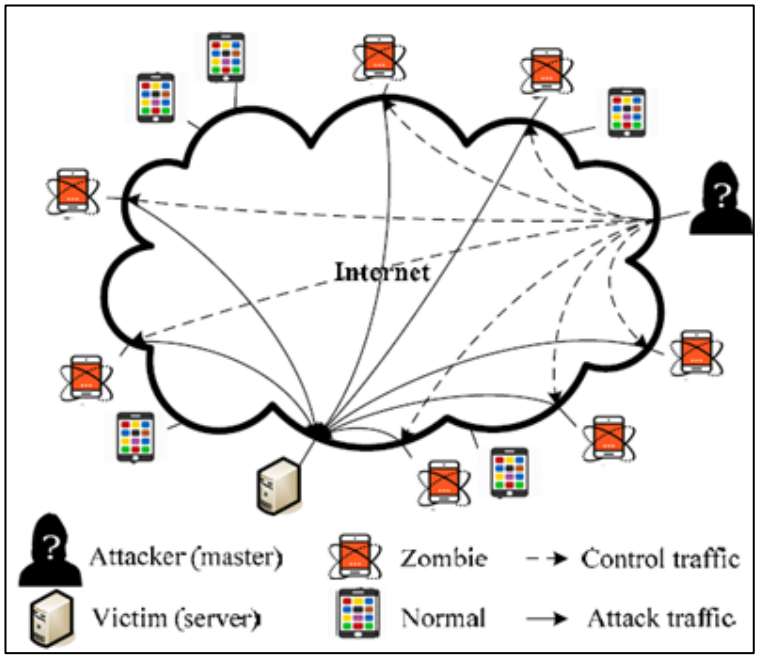

Fig. 1. DDoS attacks for Mobile devices through cloud computing

6 Proposed Model for Securing Mobile Systems against DDoS

Securing users' information and apps from attacker and hackers are a key to establish and maintain consumers' trust in the mobile platform, especially in mobile cloud computing. A proposed architecture for mobile cloud computing security is shown in Figure 2. In this architecture presented we concerned with both security of mobile users and security for user information. Since mobile devices are exposed to numerous security attacks such as: DDoS and malicious programs (e.g., virus, worm, and Trojan horses) via mobile vulnerability. On the other hand, mobile users store a large amount of information and apps on a cloud computing, so they should be careful of dealing with

these data in terms of its reliability, integrity, and security. Cloud computing provides mobile users to utilize secure cloud services on the fly as pay-as-you-go manner via the Internet.

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

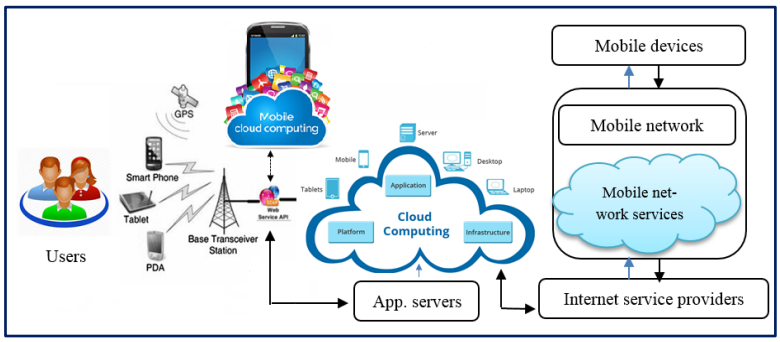

Fig. 2. Proposed architecture for mobile cloud computing security

The proposed model in Figure 3, includes various functions that define the system processes. This process are integrated to protect mobile apps against DDoS attacks. This functions produce system operations and control the constraints on each process. Some of these functions are shown in Table 1:

Table 1. Main functions to protect mobile apps against DDoS attacks

Function	Discretion
Request_controller	Used to check the "server availability"; for "Yes/No" responses action.
Unavailable_requests	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	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 "DDoS-detector" process is executed.
DDoS_detector	Used to validate the request against the DDoS attacks. If the request is not valid (i.e., No response); then the system run the "DDoS_attacks" process.
DDoS_ attacks	Used to add some flags in the request's header, these flags will be 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	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.
Mobile_cloud_services	Used to forward the results to "Check_final_response()" process.
Check_final_response	Used to validate the response, removes the processed request from the "valid_request" table, and sends the result message to the client site.

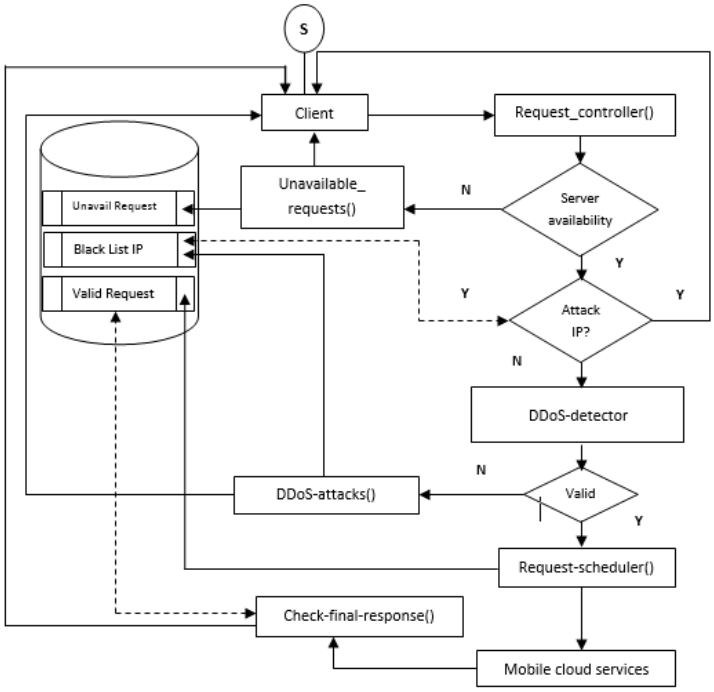

Fig. 3. Model for protect mobile-based systems against DDoS attacks

The proposed model in this research is focused to detect and protect the mobile-based systems against DDoS attacks in cloud computing environment. The performance of the updated approach was evaluated in terms of *accuracy*, *sensitivity* and *specificity* rates, which computed as following:

$$SYS_{accuracy} = (T_p + T_n) / (T_p + T_n + F_p + \boldsymbol{F}_n) \times 100\%$$
$$SYS_{\boldsymbol{sensitivity}} = (T_p) / (T_p + \boldsymbol{F}_n) \times 100\%$$
$$SYS_{\boldsymbol{specificity}} = (T_n) / (T_n + F_p) \times 100\%$$

Where, T_p is the No. of cases correctly identified as attacked packets, T_n is the No. of cases correctly identified as normal packets, F_p is the No. of cases incorrectly identified as attacked packets, and $\boldsymbol{F}_n$ is the No, of cases incorrectly identified as normal packets.

In Table 2, we have used various experimental data sizes and thresholds to get the experimental result of the proposed model. The system is evaluated under multiple source attack environments in terms of *accuracy*, *sensitivity* and *specificity*.

Table 2. Performance evaluation results

Mobile DDoS Attacks								
N	K	T_p	T_n	F_p	F_n	Accuracy	Sensitivity	Specificity
1000	150	100	900	12	6	98.23%	94.34%	98.68%
2000	200	200	1800	24	12	98.23%	94.34%	98.68%
3000	250	300	2700	36	18	98.23%	94.34%	98.68%
4000	300	400	3600	48	24	98.23%	94.34%	98.68%
5000	350	500	4500	60	30	98.23%	94.34%	98.68%
6000	400	600	5400	72	36	98.23%	94.34%	98.68%
7000	550	700	6300	84	42	98.23%	94.34%	98.68%
8000	650	800	7200	96	48	98.23%	94.34%	98.68%
9000	700	900	8100	108	54	98.23%	94.34%	98.68%
10000	800	1000	9000	120	60	96.40%	94.34%	98.68%
						98.05%	**94.34%**	**98.68%**
Performance Average								

6.1 Performance Evaluation of DDoS 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 [16], 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 F_n, we have two features fed for the implementation of algorithm; these two features are the source IP address and the destination IP address. Table 2, presents the experimental results for protect cloud systems against DDoS attacks. From Table 2, we can conclude that the system has *performance average* of (97.03%), where it has the average percentage of accuracy (98.05%), the average percentage of sensitivity (93.34%), and the average percentage of specificity (98.68%).

7 Conclusion

The main objective of this research study is to introduce a novel model for securing mobile-based systems against DDoS attacks. We present also a proposed architecture for mobile cloud computing security that concerned with both security of mobile users and security for user information. The feedbacks of the experimental results were highly promising, for protecting mobile systems against DDoS attacks. The effectiveness of the proposed approach is evaluated. For DDoS attacks detection, we have concluded that the proposed approach has *performance average* of (97.03%), where it has the average percentage of accuracy (98.05%), the average percentage of sensitivity (93.34%), and the average percentage of specificity (98.68%).

8 References

[1] Hosam F. El-Sofany, Samir A. El-Seoud, Hassan M. Alwadani, and Amer E. Alwadani, "*Development of Mobile Educational Services Application to Improve Educational Outcomes using Android Technology* ". *International Journal of Interactive Mobile Technologies* (iJIM), Vol. 8, Issue 2, Pages 12-17, http://dx.doi.org/ 10.3991/ijim.v8i2.3509, April 2014.

[2] Nirbhay K. Chaubey, Darshan M. Tank, "*Security, Privacy and Challenges in Mobile Cloud Computing (MCC):- A Critical Study and Comparison*". *International Journal of Innovative Research in Computer and Communication Engineering.* Vol. 4, Issue 2, February 2016.

[3] Mohamed Sarrab, Hadj Bourdoucen. "*Mobile Cloud Computing: Security Issues and Considerations*". Journal of Advances in Information Technology Vol. *6, No. 4, November 2015.*

[4] Puja Tekade, C.J.Shelke."*A Survey on different Attacks on Mobile Devices and its Security*". International Journal of Application or Innovation in Engineering & Management (IJAIEM). Volume 3, Issue 2, February 2014.

[5] 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.

[6] Sajedul Talukder, Iftekharul Islam Sakib, Faruk Hossen, Shohrab Hossain. "*Attacks and Defenses in Mobile IP: Modeling with Stochastic Game Petri Net*". arXiv:1804.10354v1 [cs.NI] 27 Apr 2018

[7] Mariantonietta La Polla, Fabio Martinelli, Daniele Sgandurra. "*A Survey on Security for Mobile Devices"*. IEEE Communications Surveys & Tutorials. 1553-877X/12, IEEE, 2012

[8] L. Liu, X. Zhang, G. Yan, and S. Chen, "E*xploitation and threat analysis of open mobile devices*". Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, Ser. ANCS '09. New York, NY, USA: ACM, pp. 20–29, 2009. https://doi.org/10.1145/1882486.1882493

[9] G. Kambourakis, C. Kolias, S. Gritzalis, and J. H. Park, "*DoS attacks exploiting signaling in UMTS and IMS*". Computer Communications, Vol. 34, no. 3, pp. 226–235, 2011. https://doi.org/10.1016/j.comcom.2010.02.010

[10] U. Meyer and S. Wetzel, "*A man-in-the-middle attack on UMTS*". Proceedings of the 3rd ACM workshop on Wireless security, ser. WiSe '04. New York, NY, USA: ACM, 2004, pp. 90–97. https://doi.org/10.1145/1023646.1023662

[11] M. Khan, A. Ahmed, and A. R. Cheema, "*Vulnerabilities of UMTS Access Domain Security Architecture*". Proceedings of the 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. Washington, DC, USA: IEEE Computer Society, 2008, pp. 350–355.

[12] C. Guo, H. J. Wang, and W. Zhu, "*Smart-phone attacks and defenses*". *HotNets III*. Citeseer, 2004.

[13] M. Gunasekaran, K. Premalatha, B. Gopalakrishnan. "*A Survey on DoS Attacks and Countermeasures in Mobile Ad Hoc Networks*". International Journal of Advanced Research in Computer Science, Vol.1, No. 4, Dec. 2010.

[14] Hejmo M, Mark B. L, Zouridaki C and Thomas R. K, "*Design and Analysis of a Denial-of-Service-Resistant Quality-of-Service Signaling Protocol for MANETs*". IEEE Transactions on Vehicular Technology, vol. 55, no. 3, pp. 743-751, 2006. https://doi.org/10.1109/TVT.2006.873834

[15] Xing F and Wang W, "O*n the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures*", IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 3, 2010. https://doi.org/10.1109/TDSC.2008.71

[16] 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.

[17] Final Version of NIST Cloud Computing Definition Published. Available online: http://www.nist.gov/itl/csd/ cloud-102511.cfm (accessed on September 2018).

[18] Jalaluddin Khana, Haider Abbasa, b, Jalal Al-Muhtadia. "*Survey on Mobile User's Data Privacy Threats and Defense Mechanisms*". International Workshop on Cyber Security and Digital Investigation - CSDI 2015

[19] Leung A., Y. Sheng, H. Cruickshank, "*The security challenges for mobile ubiquitous services*". Information security technical reports, Elsevier and Science Direct, 162-171, 12(2007).

[20] Roberta Cozza, "*Forecast: Mobile Communications Devices by Open Operating System",* Worldwide, 2008- 2015," Gartner, April 5,2011

[21] Ruggiero P. and Jon Foote "*Cyber Threats to Mobile*". Produced for US-CERT, a government organization, Carnegie Mellon University-US, 2011

[22] Shujithra M., G. Pasdmavati., "*Mobile Devices Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism".* International Journal of Computer Applications (0975-8887) Volume 56-No.14.

[23] E. Naone, "*SMS of Death Could Crash Many Mobile Phones*," Available: http://www. technologyreview.com/printer friendly article.aspx?id =27021, 2011

9 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. E-mail hel-sofany@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 post-graduate 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 16 October 2018. Resubmitted 29 November 2018. Final acceptance 03 December 2018. Final version published as submitted by the authors.