Indian Journal of Science and Technology, *Vol 11(15), DOI: 10.17485/ijst/2018/v11i15/119540,* April *2018*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Fog Computing: A Novel Approach to Provide Security in Cloud Computing

Abdullah AlNuaim* and Shakeel Ahmed

College of Computer Sciences and Information Technology, King Faisal University, Hofuf, Saudi Arabia;
aalnuaim2@gmail.com, shakeel@kfu.edu.sa

Abstract

Objective: Cloud Computing is the future solution which all companies in the world aim to depend on for its day to day operations because of its big advantages compared with that of the on premises systems. The major challenging issues in Cloud-based environment are security, user authentication, access control, and ensuring the security of stored data in Cloud servers which makes most of the functional and technical people to work on the aspects of security and to provide a solution to secure Cloud computing. **Methods:** Fog computing is one of the solutions created by Cisco and it is defined as the extension of the Cloud Computing paradigm, its distinctive characteristics in the location sensitivity, wireless connectivity, and geographical accessibility. Accordingly, this research offers an efficient user authentication scheme for Cloud computing by designing the user authentication and access control at the Fog level where, a client-based user authentication methodology has been introduced to confirm identity of the user at client-side to access the Cloud which will enhance the reliability and rate of trust in Cloud computing environments. The system currently being proposed is implemented on mobile devices using an application connected to a Fog node which is further connected to the Cloud node. **Findings:** In overall, the analysis of the suggested scheme shows that, designing this user authentication and access control model will enhance the security and rate of trust in Cloud computing environments as an emerging and powerful technology in various industries. **Application:** By incorporating the secured scheme of authentication, Security of Cloud computing environments can be enhanced and protect the system from unauthorized users.

Keywords: Authentication, Cloud Computing, Fog Computing, Man-in-Middle, SMS

1. Introduction

Cisco has introduced a new technology named Cloud Computing to the world upon their prior Fog Computing technology. After the introduction of Cloud computing CISCO infrastructure is extended now some of the application services that are working at the network edge in a smart device and other application services are working in the cloud in a remote data center. Figure 1 shows a framework with three level hierarchies, each smart device is linked to one of fog devices which are interconnected to each other and attached to the cloud[1].

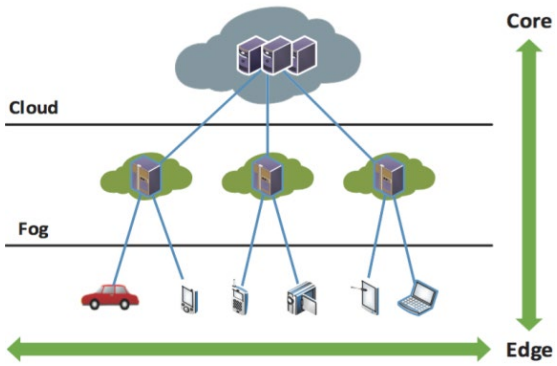

Figure 1. Framework with three level hierarchy.

*Author for correspondence

Fog is the middle layer between the source and target. The main objective of the fog is to improve the data performance which will be uploaded to the cloud for data processing, analysis and storage. Some of the properties for fog computing are: heterogeneity, location awareness and low latency, mobility and geographical distribution, large number of nodes, controlled wireless access, and streaming and real time applications[2]. In this research will produce a common issue related to fog commuting which is Man-in-the-middle attack and provide a simple and secure solution to prevent this attack with help of service provider using SMS service.

1.1 Web Spoofing

One of the middle man attack techniques is web spoofing in which people were made to believe that they are interacting with a trusted link, but in actual it's a shadow copy. The way this attack works is very simple but not easy to escape, the attackers fetches the content of a real website and mimic the content with a spoofed content, which the user is unable to differentiate, which eventually result is leaking of some personal information and data. One of the scenarios that explain web spoofing:

The attacker spoofed the user by a fake URL similar to the one which the user wants to access, by clicking on that link, which stated as http://www.domain.com but in actual it's referring to a link like http://www.attackerdomain.org, once the user enters his id and password that will be stored in attacker's database for other malicious activities, as shown in Figure 2. Solution suggested is in this paper is "Trusted Activity Chains". It's a framework level feature that provides system level defense that can be leverages by the app developers. This framework states that all the steps and or programs should run in sequence. One activity should be run at any point of time without allowing other activities to run in parallel. A lock is placed on the running activity by the system to make sure a successful execution and completion of that activity. Once the activity is completed the next activity in the uninterrupted chain of activities will be put forward for execution. This approach makes sure that any random or adhoc request or activity by the system is not executed directly or in parallel while the activities already set in the chain are being run. The advantage of using trusted activity chain is protecting any spoofing attack. When activities started, it manages until the end which it increases reliability. The big issue of using it when many activities requested at the same time, It needs many interrupt lock for managing all of the activities. It also effects on performance that activity not begin until the previous activity finished[3].

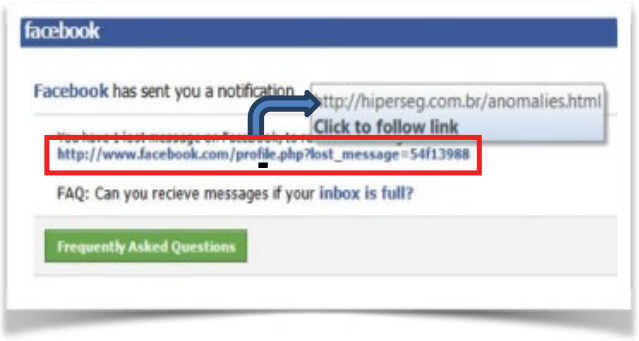

Figure 2. Web spoofing.

1.2 APR Spoofing

Another type of spoofing specially on local area network to retrieve traffic is though (APR – Address Resolution Protocol). In APR spoofing the attacker send a spoofed message on network with aim to associate his MAC address with host IP address, so the traffic will be diverted to the attacker rather to the actual user. The solution given in the paper to stop the ARP spoofing attacks is using the "Open Stack". It is open source cloud platform that uses component called comparison handler that cross checks the messages send from the handler to reliable ARP tables constructed in Keystone. This ensures the authenticity of the tables and thus discards any mismatch that happens between messages and table. The reliability increased when table contained IP and MAC address and compared with each message it matched or removed it. The issue is overloaded when ARP tables contained many IP and Mac address compared with every message that received[4].

2. Why Fog Computing

- As a middle layer between end devices and cloud, fog computing can provide additional features as an extension of cloud computing to improve data performance with other properties:
- Heterogeneity: with increasing risk of data security when directly accessing traditional cloud computing data centers, fog computing provides a virtual heterogeneous platform consisting of

computing, storage and networking services as an interface between end devices and actual cloud data centers.

- Supporting endpoints with services at network edge due to awareness and low latency in fog computing.
- Fog computing distributes the services and applications through proxies and access points.
- Fog computing supports mobility which enables the applications that are supported by fog to be communicated with mobile devices directly.
- Real-time interaction in fog computing can be used in important applications that require real-time interaction rather than batch processing.
- Fog is a form of cloud that lies low on or near ground level. Table 1 shows the differences between cloud computing and fog computing.

3. Authentication Issue in Fog

The main security issue in fog is authentication since services are provided to the end users by front fog nodes. Many authentication techniques applied for fog computing to provide an efficient authentication but some of them not efficient and have poor scalability such as Traditional PKI-based. Also biometric authentication techniques applied to provide an efficient authentication such as face authentication, fingerprint authentication, touch-based authentication or keystroke-based authentication[5].

As mentioned in[6], we need to apply an intrusion detection system to every layer to prevent any attack. One of the typical attack in fog computing which we focus to find as solution for it in this research is Man-in-the-Middle attack. The idea of Man-in-the-Middle attack is replacing the gateways that serving the fog device by fake one which is connecting to malicious access points. In this case, any private communication of victims will be hacked and thus the gateways will be controlled by the attackers. The attacker will be able to monitor and modify the data between end user and gateway. Figure 3 show an example of man-in-the-middle attack which shows the ability of the attacker to monitor and modify the data that is sending from user with a 3G connection to another user with WLAN connection in the middle of the communication. Traditional method faces difficulties to detect man-in-the-middle attack without noticeable features of this attack collected from the fog because this attack consumes a small amount of fog devices, such as memory and CPU consumption.

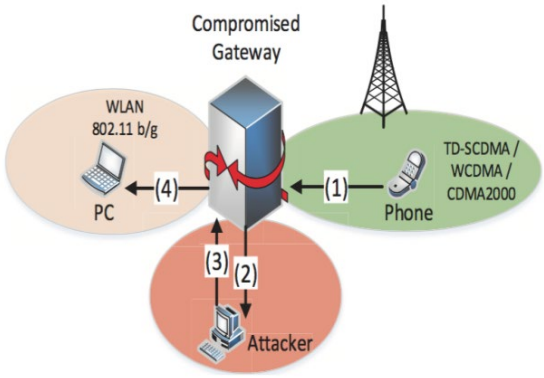

Figure 3. Man-in-the-middle attack.

Table 1. Differences between cloud computing and fog computing

Requirement	Cloud Computing	Fog Computing
Server nodes location	Within the Internet	At the edge of the local network
Client and server distance	Multiple hops	Single hop
Latency	High	Low
Delay Jitter	High	Very low
Security	Less secure, Undefined	More secure, Can be defined
Awareness about location	No	Yes
vulnerability	High probability	Very low probability
Geographical distribution	Centralized	Dense and Distributed
Number of server nodes	Few	Very large
Real time interactions	Supported	Supported
kind of last mile connectivity	Leased line	Wireless

4. Proposed Solution

This proposed solution focuses to provide a simple, less complicated and more secured solution which makes the authentication easy to manage and make access to the service easy to the end user. The solution is based on SMS service in which user mobile number is his/her unique id. In case of password, the system will generate the password with every user login and remove the password after the user logged out from the system. In this case, the user does not need to create a user name or password. Fog will be a middle layer between user and cloud in which it takes the user number and contact the cloud to generate a password randomly then send to the user through SMS service provided by service provider. Figure 4 describes how the solution is work through these steps:

- User types his/her unique mobile number, for example: 00966555555555.
- The mobile number sent from user to the Fog.
- Fog sends the number to the cloud and asks to generate a user password.
- Cloud contacts the service provider to send the password to the user as SMS message.
- The password sent to the user as SMS message.
- After typing the password by the user, the password will be sent to the Fog, and then the Fog will send the password to the cloud to check if password is match that password which is sent to the user through SMS service.
- Now the user can access the system.

The above steps show login steps for the user by generating a password randomly which will be used for one time only. After the user logged out from the system the password will be removed from the system directly and the user will not able to access to system by using same password and he should follow the login steps again to provide another new password. In this case, the fake page will not affect users because the password will be generated in the cloud and sent to the user through SMS service to user mobile.

This solution provides a simple and secured method to access a cloud system by taking the advantages of fog computing. As any other solutions, this solution has its advantages and disadvantages as we will see in this paper.

4.1 Advantages

Due to the simple and secure proposed solution we can discover these advantages:

- No need to reset password with traditional method which require answer question and many steps or two step authentication, the password will reset automatically with every login.
- Creating an account will be easy and does not need much information except that information which are needed as requirements of process.
- There is no attack even if you enter your mobile number in fake page. The fake page will be not connected to the real server to generate a password for the user as shown in Figure 5.

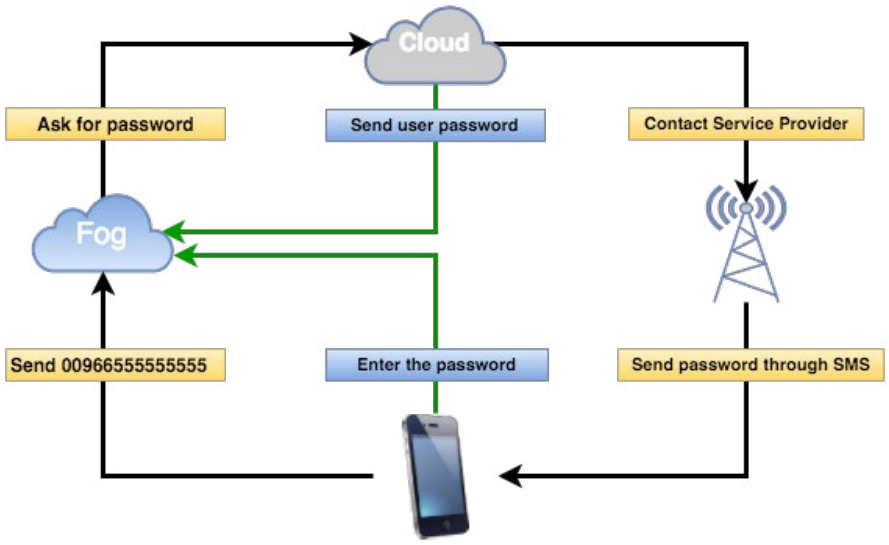

Figure 4. Login steps.

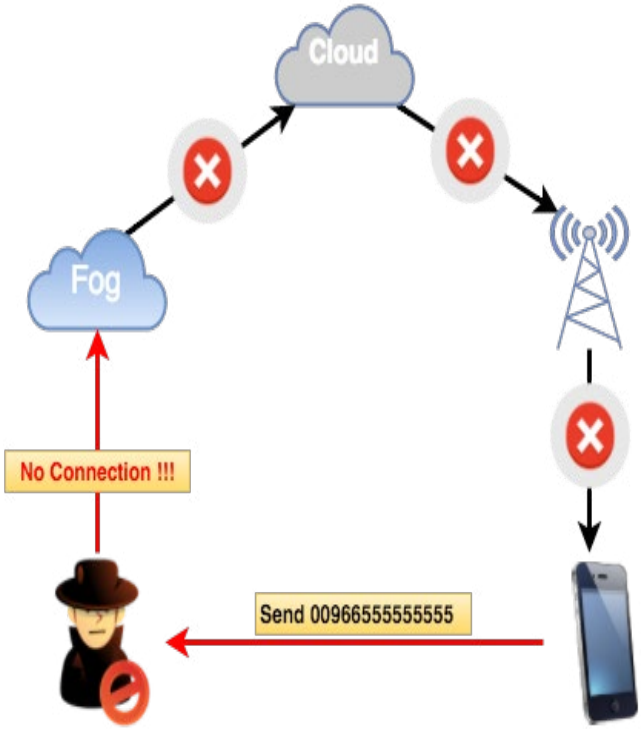

Figure 5. Login through fake page.

- The user number will be unique globally such as 0096655555555 which are related to someone in Saudi Arabia.
- This number prove yourself (authentication): Your password will be sent to your number which is your unique id. In this case your number will be your user name and your authentication to access and this advantage provide the simplicity in addition to security.
- No need to remember your password because it will be always changed with every login and log-out process.
- Easier to use by user, manage by admin and implement by developer. The admin will not need to track every ID and reset the password; the resetting will be automatically by the system. In case of developer, he will not need to create a huge database table contains an information such as static password, users' questions and answers or other fields related to user authentication. The password field will be updated automatically during login and logout duration.

4.2 Disadvantages

Any solution has its disadvantages which we can discover it to improve the solution in the future:

- Signals of phone by service provider should be covered in the area in which you are try to login in to the system.
- You must be connected to the internet, but should consider this as disadvantage? The cloud and fog depending on the internet servers, so without the internet you cannot use the service at all not only access to the serves.
- Your phone should be always with you; it is your password. Steal the phone means steal your password, so you need to protect your phone by using password. Some of smart phone company provides such services such as lock or delete you phone remotely, so we can get benefits from these services. And of course our local data more important than our data in cloud, so everyone able to use fog or cloud service should be able to use these company services and should be able to lock the phone remotely.
- Moving SIM card to another phone: another case of stealing the phone is to move the SIM card to another phone and the only solution is to protect your SIM card by password and in worst case you should call service provide to lock your SIM card and extract another one.

5. Conclusion

Fog computing is an extended cloud for smart devices working at edge of the network which aims to process and analysis data before sending to the cloud. Fog stays in the middle between devices and cloud in which it can provide more secure and private communication with other additional features that are not included in the cloud. In our research we focused on the main issue faced the fog which is man-in-the-middle attack. This attack enables the attacker to replace the service that serve specific device with fake one. We proposed a simple and secure solution to prevent this kind of attack using SMS service. The idea not to prevent the attack only, also if the end user faced a fake page, he will not

be affected because the password will be generated with every login and deleted with every logout. The attacker will not get any benefit from his fake page because the fake page will not be connected to the cloud and password will generated in the cloud and sent to the user through SMS service by service provider. This solution can be improved in the future with other features, for example: Set a specific time for step 6 in case of another attack may happen in this duration.

6. References

1. Stojmenovic I, Wen S. The Fog computing paradigm: Scenarios and security issues. Federated Conference on Computer Science and Information Systems; Warsaw. 2014. p. 1–8. crossref
2. Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the Internet of Things. Proceedings 1st Edition MCC Workshop Mobile Cloud Computing; 2012. p. 13–16. crossref
3. Boureanu I, Owesarski P, Vaudenay S. Applied cryptography and network security. Springer International Publishing Switzerland; 2014. p. 494–512. crossref
4. Kang HS, Son JH, Hong CS. Defense technique against spoofing attacks using reliable ARP table in cloud computing environment. Network Operations and Management Symposium (APNOMS); 2015. p. 592–5. crossref
5. Yi S, Qin Z, Li Q. Security and privacy issues of fog computing: A survey. Wireless Algorithms, Systems, and Applications. Springer; 2015. p. 685–95. crossref
6. Yi S, Hao Z, Qin Z, Li Q. Fog computing: Platform and applications. 2015 3rd IEEE Workshop on Hot Topics in Web Systems and Technologies; 2015. p. 73–8.