Secure and Strong Mobile Cloud Authentication

[1]Qassim Bani Hani, [2]Julius P. Dichter
Department of Computer Science & Engineering
University of Bridgeport, CT-06604
[1]qbanihan@my.bridgeport.edu, [2]dichter@bridgeport.edu

Abstract—Mobile cloud computing has dual benefits that includes cloud computing and mobile computing. In mobile cloud computing data storage and data processing take place outside the mobile device. As a result, there is a high chance of security attack. The security even becomes more critical when mobile phone is initiating the handoff during handover management process. Thus, the attacker may easily get access to our sensitive data. Due to this the malicious user may see or modify our data. In order to overcome this problem, we need to store our data in clouds in a secured manner. In this paper, we propose a secure and strong authentication (SSA) process that stores the key at different cloud servers. This process provides strong authentication. Greencloud is used to validate the process. The results confirm that our proposed SSL protects the mobile cloud computing from malicious activities.

Keywords—Mobile cloud computing; Authentication; Greencloud; Secure and Strong Authentication; Accuracy; Reliability

I. INTRODUCTION

Now-a-days the usage of mobile devices increases rapidly, about 95% of the people are using mobile devices particularly smart phones [1].The smart phones provide several utilities such as short message service (SMS), multimedia message service (MMS) and videos [2]. The mobile phone provides the mobility support to move from one network to another network rapidly as this feature meets our needs. On the other hand, it provides the platform for adversary to attack on our sensitive data [3-5]. Furthermore, there is high possibility to slow down the service [6].

Generally, the mobile computing architecture consists of "Radio Sub System (RSS), Network Sub System (NSS) and Operating Sub System. In RSS all the mobile stations are connected to base station sub system. In NSS all the base station controllers are connected to mobile controller [7]. The operations Support Systems (OSS) consists of an authentication center that controls the NSS and RSS. There are several possible attacks expected on the mobile cloud computing such as privacy, integrity, and authentication [8].

In mobile computing the large data is stored in the cloud servers. Here, we have to consider three factors: the mobile cloud should securely store the data, the data should be transferred correctly and finally data should be received by the correct user [9]. Handling to these three factors are cumbersome process. Thus, transferring data from the cloud to mobile devices face the problem of malicious users that can exploit the confidential and sensitive data.

Limiting the access of adversary to mobile cloud computing, there is need of strong authentication process. Here, we propose secure strong authentication process based on One-time password (OTP). In this process, the user information is forwarded to cloud owner prior to accessing the mobile cloud that helps to identify the authenticity of the user. If the mobile cloud user is authenticated then OTP is sent for accessing the cloud otherwise, the access is denied. Our proposed approach protects the mobile devices against authentication attacks. In our proposed approach, we store the key on different mobile clouds, so it is difficult to the attacker to break the key. This process secures the data in the cloud servers by providing strong authentication. The remainder of the paper is organized as follows: Section II discusses the some of the related interesting approaches. Section III presents proposed secure and strong authentication process based on One-time password. Section IV gives experimental results and finally entire paper is concluded in section V.

II. RELATED WORK

In this section, the salient features of existing approaches are discussed. Flexible framework is proposed in [10] to provide the authentication. In this framework, trust and usability are managed using flexible policies and dynamic revolving. This framework involves the TrustCube called as authentication infrastructure management and behavioral authentication.

In [11], light weight protocol is introduced to generate dynamic credential to protect against powerful attackers that steal the user credentials, such as digital certificates, and passwords.

Strong user authentication framework is proposed for mobile cloud computing [12]. In this framework, user validity is strongly confirmed before enter into the cloud. The framework provides identity management, session key establishment and mutual authentication between a user and the cloud server. In this approach user is authorized to update its user name or password whenever necessary.

Elliptic Curve Cryptosystem (ECC) dynamic ID-Based remote mutual authentication approach is proposed [13] for remote devices to handle the authentication process.

The mobile cloud data processing framework is introduced in [14]. The framework is based on trust management and private data segregation. Focus Drive is used to demonstrate the proposed solution. All existing approaches are addressing the mobile cloud computing, but their focus on providing the

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

framework to handle the authentication process at the server side. However, our proposed protocol addresses the secure authentication at the client side during the mobility.

Algorithm 1: Secure and strong authentication process

1. Initialize: (U_i= user, O_i = owner, A_s = authentication server, C_s = cloud server)
2. User requests => owner
3. Owner sends => authentication server
4. Authentication server gives token => user
5. User maps token to cloud server
6. Cloud server access
7. Key $_1$ =>C_{s1}
8. Key $_2$ =>C_{s2}
9. Key $_3$ =>C_{s3}
10. Get access to the resources

III. Secure and Strong Authentication Process

In order to keep the data more secure, we designed a secure and strong authentication process. For strong authentication first we have to make a strong key, for the strong key we use SSA algorithm to encrypt the data. The cloud owner only has the idea about the encryption algorithm. After encryption, the key is stored on different cloud servers by splitting, so when the attacker wants to break the key it is very difficult to get each piece of the key from the different cloud servers. Even if the attacker gets all the pieces of the key then it is not capable to understand the pattern of the keys. By following this strong authentication process, we can easily secure our sensitive data from the malicious users in the mobile cloud computing.

In this strong authentication process when user wants to get access to the data, he/she has to get the key from the owner. The process to get the key is explained in algorithm 1.

Firstly, the user requests the cloud owner to use the data present in the cloud server. Then the cloud owner collects the owner data and sends that to the authentication server that checks whether the user is legitimate or not and sends token to the user, if the user is legitimate. Then the user sends the token to the cloud server the cloud server checks the information and generates key for the user, if the user is not the correct person then it sends information to the owner. Then owner knows that some attacker is trying to get access to his sensitive data and stops the process. When the key from the user matches to the cloud server then it provides access to the user to use the resources. The complete secure authentication process is depicted in Figure 1.

In strong authentication algorithm when user$'U_i'$requests the owner $'O_i'$for the resources, then the owner sends the information of the user to the authentication server $'A_s'$. As authentication server checks whether the user is legitimate or not and generates token for the user. Through the token, the user gets access to the cloud server. After getting the access to the cloud, the user gets the data whatever requires. This is strong enough process to break the security.

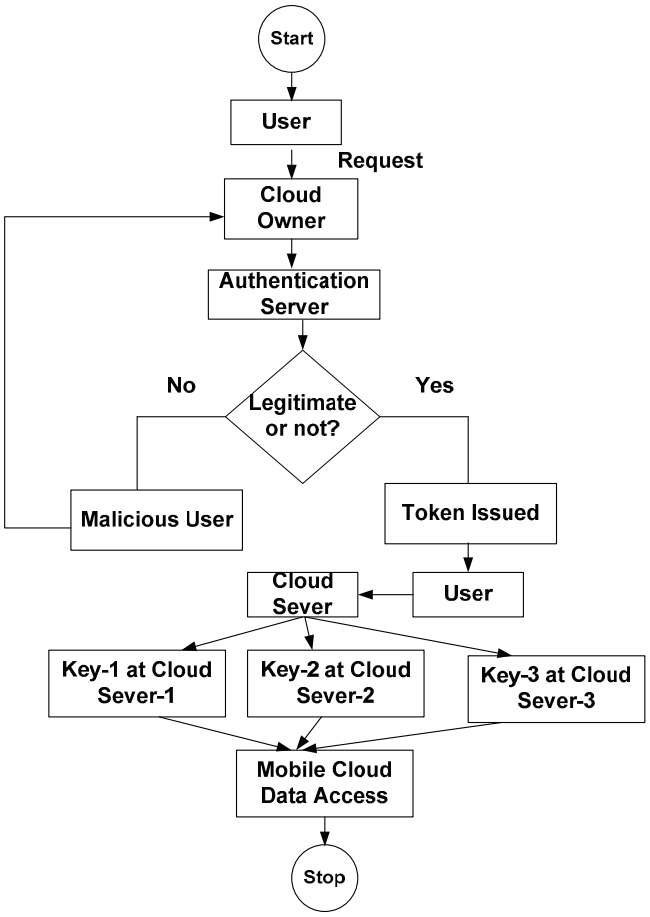

Fig. 1. Secure strong authentication process for mobile cloud computing

IV. Experimental Results

To show the effectiveness of the proposed secure and strong authentication approach, we tested the SSA in different scenarios. The system model is programmed with C++ and tests are conducted on the GreenCloud simulator. The GreenCloud simulator is installed with Ubuntu 13.10 Operating system. The experiments are conducted on a laptop with 2.8GHz Pentium Dual Core CPU and 5 GB RAM. The test machine uses the 64-bit version of Windows 8.

We generated data center supported scenarios. The network size consists of 1200 X 1200 square meters. We use 1860 chassis switches, 1456 line cards and 46 ports in the core layer. In the aggregation layer 214 chassis switches, 123 line cards and 48 ports are used. Data center is used by maximum 13200users.

Each user performs maximum 19 tasks/second. The size of each task is 10500 Bytes. Data center network is supported with 5 layer-3 (core layer), 125 layer-2 (aggregation layer) and 118 hosts are available in each rack. Each host has a support of 8 processors with 64 GB Memory, 180 Storage and 208 virtual disk size. The positions of the Switches are set very interestingly. As, Layer-3 is set at center of the network with X-axis, but Y-axis is set at 550 and Z-axis at 0.

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

Different bandwidth is set from layer-1 to Host layer. Layer-1 to Layer-2 has 180 GB, layer-2 to layer-3 has 50 GB and layer-3 to host layer has 3.5 GB. Priority queue with drop tail queue is used for buffering the packets. However, queue delay is negligible that cannot affect the transmission, but burst time and idle times are set 678 msec and 49 msec respectively. At transport layer, TCP SACK is used separately in two different simulation times.

The packet size is set 1250. The initial congestion window is set to 1 IMSS that is equivalent to 32. Slow start threshold is set 512 and Maximum congestion window size is 1024. The simulation time for this processing is set 112.5 seconds. The size of output task should not extend more than 280500.These results have been used in the MATLAB to show the effectiveness of our proposed approach. Based on the results, we have selected some of the interesting metrics.

- Accuracy
- Reliability

A. Accuracy

Accuracy is considered as the basic step to measure the performance of any proposed model. It is also used as obvious criterion for prediction. Here, we generated 1000 attacks including 8000 legitimate messages to determine the accuracy of the proposed algorithm.

Accuracy of our proposed SSA is calculated as

$$A_{SSA} = \frac{T_n + T_P}{T_n + F_p + F_n + T_P} \qquad (1)$$

Where

A_{SSA}: Accuracy of Secure and strong authentication algorithm; T_n: True negative; T_P: True positive ; F_p: False positive and F_n: False negative.

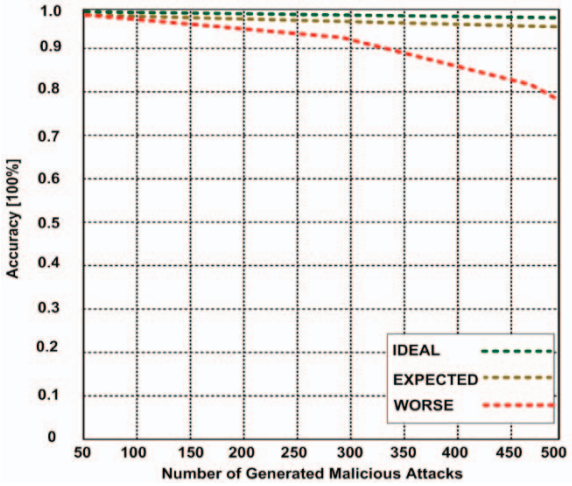

Fig. 2. Accuracy with moderate number of generated malicious attacks

We evaluated SSA using three cases: Ideal case, Expected case and worse case scenarios. We observed from the Figures 2 that number of generated attacks do not highly affect the accuracy of our proposed SSA algorithm, but accuracy is declined in the worst case scenarios.

Furthermore, In Figure 3, accuracy of expected and ideal scenarios remain constant, but only accuracy is affected in worst case scenario. In idea case scenario, the accuracy is counted to 99.8% because we did not have congestion on the network and each malicious attack is generated after 50 milliseconds so that our approach has enough time to detect the threats. On other side, we created each attack after 30 milliseconds in expected scenario. However, our scheme is capable to detect the threats and accuracy remains 98.3%. In worst case scenario, we generated attacks after each 1 millisecond that highly affects the results and obtained overall 74.2% accuracy. We believe that our proposed approach will perfectly works for expected and ideal scenarios.

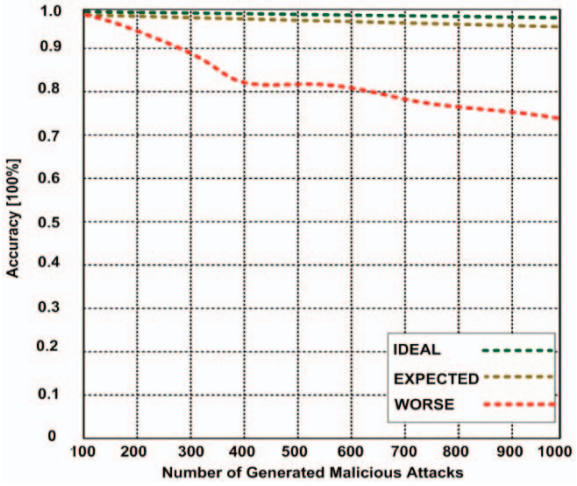

Fig. 3. Accuracy with higher number of generated malicious attacks

B. Reliability

The reliability is the key factor to determine the authentication of any proposed approach SSA. In Figure 4, we determined the reliability of our proposed approach and compared with other known authenticating provisioning approaches: Secure Data Processing (SDP) [14], Energy-Efficient Incremental Integrity (EEII) [15], and TrustCube Authentication (TCA) [16].

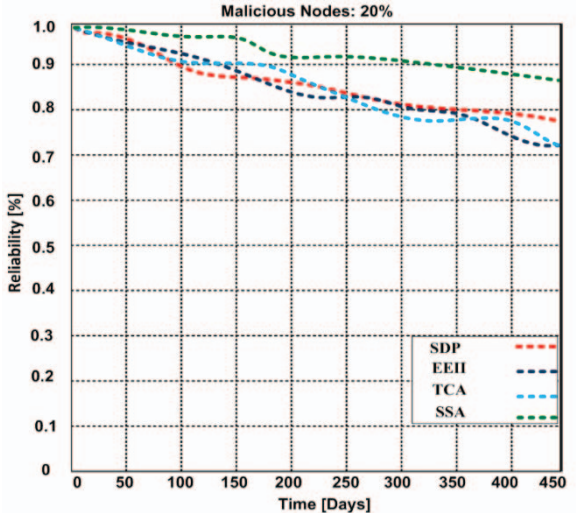

Fig. 4. Reliability VS Time in days

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

In this experiment, we generated 20% malicious nodes to find the suitability of the approaches. Based on the results, we observed that when number of days increase, the reliability of all approaches start reducing. However, our approach is less affected as compared with other approaches. The results show that our approach is 8.4- 15.1 % more reliable than other approaches.

The reliability is determined by applying following formula.

$$R = \sum_{j=1}^{N} \frac{j(S_c \times 100)}{\beta} \quad (2)$$

Where R: Reliability of the proposed system; S_c: Successful communication and β: Generated threats.

V. CONCLUSION

In this paper, secure and strong authentication algorithm is proposed for authenticating the mobile user in the mobile cloud computing environment. In proposed algorithm, secret encryption key is made split and stored on different cloud servers. The SSA protects the mobile cloud users against the malicious activities. Our proposed SSA is validated using Java platform. In this paper, we generated three different scenarios: Ideal, expected and worst. The results demonstrate that our proposed SSA is highly effective in ideal and expected situation. It can provide strong and secure authentication against malicious users and its generated attacks. SSA also helps maintain the privacy of the mobile cloud users. In future, we extend our SSA algorithm to determine its computational complexity in mobile cloud environment.

REFERENCES

[1] Samad J, Loke SW, Reed K. Mobile Cloud Computing. Cloud Services, Networking, and Management. 2015:153-90.

[2] Nkosi MT, Mekuria F. Cloud computing for enhanced mobile health applications. InCloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on 2010 Nov 30 (pp. 629-633). IEEE.

[3] Kumar K, Lu YH. Cloud computing for mobile users: Can offloading computation save energy?. Computer. 2010 Apr 1(4):51-6.

[4] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation computer systems. 2012 Mar 31;28(3):583-92.

[5] Rizvi, Syed, Abdul Razaque, and Katie Cover. "Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment." *Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference on*. IEEE, 2015.

[6] Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB. An analysis of security issues for cloud computing. Journal of Internet Services and Applications. 2013 Dec 1;4(1):1-3.

[7] S.K.Sood, "A combined approach to ensure data security in cloud computing", in S.K. Sood/Journal of Network and Computer Applications Vol.35, pp. 1831–1838, 2012.

[8] Ko SK, Lee JH, Kim SW. Mobile cloud computing security considerations. Journal of Security Engineering. 2012 Apr;9(2).

[9] Chetan S, Kumar G, Dinesh K, Mathew K, Abhimanyu MA. Cloud computing for mobile world. available at chetan. ueuo. com. 2010.

[10] Rizvi, Syed, Abdul Razaque, and Katie Cover. "Cloud Data Integrity Using a Designated Public Verifier." *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on*. IEEE, 2015.

[11] Xiao S, Gong W. Mobility can help: protect user identity with dynamic credential. InMobile Data Management (MDM), 2010 Eleventh International Conference on 2010 May 23 (pp. 378-380). IEEE.

[12] Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H. A strong user authentication framework for cloud computing. InServices Computing Conference (APSCC), 2011 IEEE Asia-Pacific 2011 Dec 12 (pp. 110-115). IEEE.

[13] Chen TH, Yeh HL, Shih WK. An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing. InMultimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on 2011 Jun 28 (pp. 155-159). IEEE.

[14] Huang D, Zhou Z, Xu L, Xing T, Zhong Y. Secure data processing framework for mobile cloud computing. InComputer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on 2011 Apr 10 (pp. 614-618). IEEE.

[15] Itani, Wassim, Ayman Kayssi, and Ali Chehab. "Energy-efficient incremental integrity for securing storage in mobile cloud computing." Energy Aware Computing (ICEAC), 2010 International Conference on. IEEE, 2010.

[16] Chow R, Jakobsson M, Masuoka R, Molina J, Niu Y, Shi E, Song Z. Authentication in the clouds: a framework and its application to mobile users. InProceedings of the 2010 ACM workshop on Cloud computing security workshop 2010 Oct 8 (pp. 1-6). ACM.

978-1-4673-8460-5/16/$31.00 ©2016 IEEE