An Enhanced Authentication Strategy for Multiservice Authorization over Mobile Cloud

Mr. Falesh M. Shelke
M.E. 4th Sem Computer Science and Engineering
P.R.Patil College of Engineering
Amravati, India
falesh123@gmail.com

Prof. Pravin D. Soni
Prof. Department of Computer Science and Engineering
P.R.Patil College of Engineering
Amravati, India
pravindsoni@gmail.com

***Abstract*—** Over the past decade the enterprise computing has been shifted to new paradigm called as Cloud computing. The cloud-computing paradigm provides several service models fitting the needs of an individual or organization. The ease of deployment, reduced costs, availability, scalability, accessibility, flexibility and location independence are some of the very strengths of this paradigm, giving rise to its popularity. Another emerging trend in enterprise computing is the use of smart phone devices, the Smart phone devices has been advanced greatly, in recent years, so has malicious code. Although, smart phones are advancing in terms of computational power, rapidly replacing Personal Computers (PCs) as first choice of a computing device but there is a major problem of resource poverty. For overcoming that issues now most of the organizations started to providing cloud services to their users. This flexibility and accessibility increases the popularity of Mobile cloud computing. On the contrary, security and privacy issues are limiting its wide spread deployment. This paper introduced a new Authentication Strategy for a mobile cloud, Which will provide high security while accessing the number of services provided by the cloud. The propose system overcomes the issue of stealing the authorization tokens through malicious insiders by using a multi tokens as well provides a security against Eaves Dropping and Man In Middle attack.

Keywords: *Cloud Computing , Mobile Cloud Computing, Smart phone, Authorization*

*****

I. INTRODUCTION

Over the past decade, enterprise computing has been shifting to a new paradigm, namely the cloud computing. The cloud-computing paradigm provides several service models fitting the needs of an individual or organization. The ease of deployment, reduced costs, availability, scalability, accessibility, flexibility and location independence are some of the very strengths of this paradigm, giving rise to its popularity. On the contrary, security and privacy issues are limiting its wide spread deployment. Organizations are hesitant to storing and communicating valuable enterprise information to a third party outside their premises. In particular, the threat of unauthorized access to cloud data is of great concern, prompting researchers to propose novel authentication mechanisms. One such method is the deployment of a centralized Identity Management System. Another emerging trend in enterprise computing is the use of Smartphone devices. International Data Corporation reports on 33% increment trend on the sale of smart phones during past few years, with a prediction of 32.7% increase in 2013 [1].

Smart phone devices has been advanced greatly, in recent years, so has malicious code [2]. Although, smart phones are advancing in terms of computational power, rapidly replacing Personal Computers (PCs) as first choice of a computing device [2], Nonetheless, their major problem still is that of resource poverty. To cater with this problem, organizations have started providing access to cloud services for their users with smart phone-based clients [3][4]. The location independence and computing power of a cloud joined with the mobility of a smartphone gives the freedom of computing anything anywhere, resulting in a powerful ubiquitous computing model. This power and flexibility is bringing high popularity to what researchers call Mobile Cloud Computing (MCC) [5][6]. ABI Research estimates that MCC will gain a user-base of 240 million by the end of 2015 [7].

Being very convenient and accessible, smart phones are at a higher security risk than competing devices. This risk is mainly because of inherent nature of their application software and communication mechanism [2], as we explain further. First, tiny applications are easy to build by anyone, thus freely available, and hence contain malicious code in several instances. Second, mobile software development life cycle does not provide any activities ensuring the security, safety and trust. Third, the constrained resources do not allow executing full antivirus software. Fourth, the inherent nature of wireless links available to eavesdropping, and the wider availability of Internet, even out of enterprise perimeter to access enterprise data leaves valuable information asset on risk. Fifth, the mobile users choose relatively simpler passwords that are easy to type with constrained input methods [5].

For all aforementioned reasons, strong authentication mechanisms for MCC are needed to protect privileged organizational data. In general, organizations deploy an IdM for greater access control, both for mobile based and PC-based client.

2. LITERATURE REVIEW

2.1 Two Factor Authentication (2FA) :

Choudhury, A.; Kumar, P.; Sain, M.; Lim, H. and Hoon Jae-Lee proposed a method which uses Two Factor Authentication (2FA) where first the tenant gets verified by a password and smart card and then is authenticated by Out Of Band (OOB) authentication. Drawback of this work is smart card as login is prone to get stolen. For the messages sent from A to S are only related with secret data stored in the smartcard, the attacker can impersonate as a legal tenant. The attacker can compute intermediate values. Therefore, the messages in login phase authentication phase can be generated by the attacker so that the attacker can successfully create a valid login request as a legal tenant. Moreover, this method uses One Time Passwords (OTP)/OOB that is prone to phishing attacks [8] and clock has to be synchronized from time to time with the server.

2.2 Authentication using graphical password in cloud:

Guo, M.; Liaw, H.; Hsiao, L.; Huang, C.; and Yen, C. proposed a method in which Tenants are also authenticated using graphical passwords. The algorithm works as the tenant is made to select one image from multiple images and then tenant draws a correct pattern to get authenticated [9]. This algorithm is prone to shoulder surfing attacks. Another problem is the images are stored locally so if the device crashes, authentication would not be possible.

2.3 Trust Cube :

Richard et al. [10] proposed Trust Cube which is an independent policy-based cloud authentication platform using open standards with the integration of various authentication methods. This model addresses the authentication issue in a simple and flexible manner by considering various sources such as device integrity reports, user credentials, etc. It uses federated authentication framework (OpenID) which uses star-shaped topology. A star-shaped topology also has privacy benefits, as only the center of the star needs to collect user-specific data. In a star-shaped topology, there are potentially heavy loads on the authentication service due to its central role in the process.

2.4 Authentication Based on Clients Personal Data:

R.Chow et al. [11] present authentication platform in which behavioural authentication is used based on client personal data. The cloud authentication platform responds to the client access request based on decision obtained by processing behavioural data of the authenticated client, however, passing the personal information of the client to cloud can affect the user privacy.

2.5 Secure cloud storage for conventional data archive of smart phones :

Hsueh et al [12] proposed authentication mechanism in which mobile device encrypts the credential information file and stores it on cloud but infected cloud server can steal the user credential information by decrypting user's files.

2.6 Secloud:

Saman Zonouz et. al. [13] proposed Secloud; a cloud based comprehensive and lightweight security for smartphones. Secloud runs the emulators of Smartphones in cloud which provide security to mobile device by security analysis of data in mobile device. In this architecture cloud assumes to be fully trusted which needs to be reconsidered .The personal data of users accessed to the cloud can affect the privacy issues.

3. SYSTEM IMPLEMENTATION AND WORKING

As our main area of discussion is to provide security for the services provided by cloud. For that I have developed a Enhance authentication strategy for multiservice authorization over mobile cloud. In this system firstly user has to Registered over a cloud via our application with the help of Signup page by inserting the information like Password, Contact number and Profile, don't need to insert username.

In this application to provide more security takes IMEI number of a Smart phone due to that no same username will be allowed. After that user has to login into his/her account for accessing the services, once the user get logged in into his/her account he/she has to select a service which needed. Once the user selects the service application generates the ticket to access the specific service. If the user granted for the services then he/she able to access the same service otherwise user get logged out due to violation of the ticket. For the ticket generation, authentication and granting access I have implemented Kerberos. This Application will helps the user to avoid Man In the middle attack as well the attacks via proxy's. Proposed System consist of three modules which is shown in following Diagram

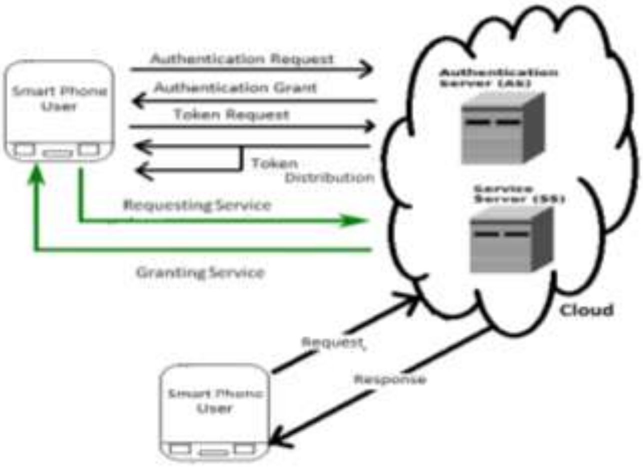


Fig. 1 system Architecture

I. Android Application

First module is the android smart phone application which will have to install on a users smart phone. This android application contains the login page where user can log in into our system by entering username and password. If the user is new then user can signup onto our application via filing a small registration form. This application is used for Singing in into account and Accessing the various Services.

II. Authentication Server

This module is implemented for the authentication purpose. This will checks the authenticity of a user by checking his/her username and password. This Authentication Server is implemented by using Kerberos.

Kerberos Authentication:

Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

III. Service Server

This module is implemented to provide the requested services to the client. this module checks the tickets which are send via user to the service server after performing authentication request-grant and token i.e. ticket request-distribution process. Once the request for a service from the user is received it checks whether the user having a authority to access the service or not, if yes then user can access the service otherwise user get logged out.

Working :

1) User has to Sign up to the application by filling registration form.
2) User has to log in into application by inserting password, it takes username as IMEI number of a smart phone by default to provide more security.
3) When the user clicks on sign in button, it will firstly sends the authentication request to authentication server.
4) If the authentication is granted, it will sends the request for generating tickets otherwise it logged out the user
5) Once the ticket is generated this ticket sends to user for accessing the services.
6) After that user has to select the service and have to click on Grant the service button
7) It sends same ticket to the Service Server for accessing the service; service Server will check this ticket.
8) If the ticket gets matched, User gets the access to the service otherwise user gets logged out.

IV. RESULT ANALYSIS

4.1 Security

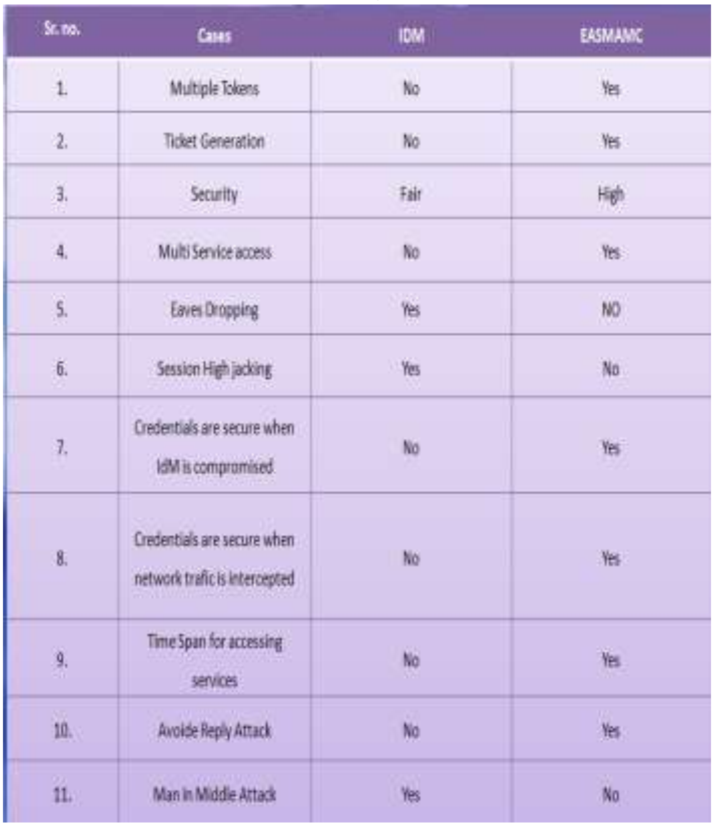
This system implements more security because in this system, it takes the IMEI number as a username. As we know that every smart phone contains its own IMEI number which is unique for each. When user wants to log in then he/she just have to insert the password, the username will taken as default IMEI number.

For providing more security System will apply SHA1 algorithm to convert password into hash code. So that Attacker can’t guess the password correctly.

4.2 Authentication Strategy

This system implements the Kerberos Authentication; Basically Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It aimed primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

Table 1. Result analysis with present IDM



Sr. no.	Cases	IDM	EASMAMC
1.	Multiple Tokens	No	Yes
2.	Ticket Generation	No	Yes
3.	Security	Fair	High
4.	Multi Service access	No	Yes
5.	Eaves Dropping	Yes	NO
6.	Session High jacking	Yes	No
7.	Credentials are secure when IdM is compromised	No	Yes
8.	Credentials are secure when network trafic is intercepted	No	Yes
9.	Time Span for accessing services	No	Yes
10.	Avoide Reply Attack	No	Yes
11.	Man In Middle Attack	Yes	No

V. CONCLUSION & FUTURE SCOPE

Thus this paper introduced a new Authentication Strategy for a mobile cloud, Which will provide high security while accessing the number of services provided by the cloud. This system overcomes the issue of stealing the authorization tokens through malicious insiders by using a multi tokens as well provides a security against Eaves Dropping and Man In Middle attack.

In a future the system can be implemented with link to link encryption in which whole packet will encrypted. Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted.

REFERENCES

[1] Ahmad, A.; Hassan, M,M; Aziz, A.; "A Multi-Token Authorization Strategy for Secure Mobile Cloud Computing", Conference on Mobile Cloud Computing , 2014 IEEE, pp.136-141, Feb 2014

[2] I. Bernik and B. Markelj, “Blended threats to mobile devices on the rise,” in 2012 International Conference on Information Society (i- Society), 2012, pp. 59 –64.

[3] R. G. Chicone, An Exploration of Security Implementations for Mobile Wireless Software Applications within Organizations. Minneapolis: Graduate Faculty of the School of Business and Technology Management, Northcentral University, 2010.”

[4] “ M. K. Riedy, S. Beros, and H. J. Wen, ‘Management Business Smart Phone Data’ in Journal of Internet Law, pp. 3- 14,2011.”

[5] F. Liu, P. Shu, H. Jin, L. Ding, J. Yu, D. Niu, and B. Li, “Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications,” *IEEE Wireless Commun ications*, vol. 20, no. 3, pp. 14–22, 2013.

[6] Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, “Heterogeneity in mobile cloud computing: Taxonomy and open challenges,” *IEEE Communications Surveys Tutorials*, vol. Early Access Online, 2013.

[7] “https://www.abiresearch.com/research/product/1005283-mobile-cloudapplications”

[8] Choudhury, A.; Kumar, P.; Sain, M.; Lim, H. and Hoon Jae-Lee, "A Strong User AuthenticationFramework for Cloud Computing", Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, pp.110-115, 12-15 Dec. 2011.

[9] Guo, M.; Liaw, H.; Hsiao, L.; Huang, C.; and Yen, C., "Authentication using graphical password in cloud", Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on , pp.177-181, 24-27 Sept. 2012.

[10] Richard Chow, Markus Jakobsson, Yuan Niu, Elaine Shi, Yuan Niu, Zhexuan Song,“Authentication in the Clouds: A Framework and its Application to Mobile Users”,CCSW’10, ACM, 2010, 978-1-4503-0089-6/10/10, pp. 1-6.

[11] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi and Z. Song,” Authentication in the clouds: a framework and its application to mobile users,” in Proceeding ACM Cloud Computing Security Workshop, CCSW ’10, Chicago, USA,Oct. 2010.

[12] S.C. Hsueh, J.Y. Lin and M.Y. Lin,” Secure cloud storage for conventional data archive of smart phones “ in Proceeding 15th IEEE International Symposium on Consumer Electronics ,ISCE ’11, Singapore, June 2011.

[13] Saman Zonouz, Amir Houmansadr, Robin barthier, Nikita Borisov, William Sanders,”Secloud:Acloud based comprehensive and lightweight security solution for smartphones,” published in Science Direct journal of Computers and security ,Volume 37, 2013, pp. 215-227.