International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 15 (2018) pp. 11810-11815

Securing Data using Touch Stroke Authentication in the Mobile Cloud

Ramananda Mallya K
Research Scholar, Bharathiar University, Coimbatore
Information Science & Engineering Department
MITE, Moodbidri, Karnataka, India

Dr B Srinivasan
Department of Computer Science
Gobi Arts and Science College
Gobichettipalayam, Tamilnadu, India.

Abstract

Mobile Cloud Computing is the rapidly growing technology in the field of Information Technology, which enables the users to rapidly get connected to the Cloud using Smart phones. Security is identified as a major issue of concern in the implementation of Mobile Cloud. One major security problem in the implementation of Mobile Cloud is the Authentication of user, who wishes to connect to the Cloud. Integrity and Confidentiality of data and user have to be given highest importance, without negotiating the user convenience provided by the Smart phones. This paper gives an overview of the Mobile cloud computing concepts, the related security issues and then proposes a secure touch stroke based Authentication method for M-learning application in the Mobile Cloud.

Keywords: Cloud Computing, Mobile Cloud Computing, Authentication, Data Security, Touch Stroke Dynamics

INTRODUCTION

Today's Mobile technology is the key in achieving cost-cutting schemes being used in modern institutions. Companies have started to allow the employees to bring their own devices to access company data [1]. The convenience and easy to use technology offered by today's Smart phones has opened up a wide range of uses and applications related to modern industries. One of the major technologies employed by the modern industries involving the Smart phones is Mobile Cloud Computing.

Mobile Cloud Computing is the hot research issue in industries and among the researchers, having many advantages such as convenience and ease of access [2]. This new technology has turned internet into a separate and vast computing field, having a bright prospering future. The uses of this technology has covered almost every area including education, e-mail, healthcare and Information technology.

In the education scenario, the institution data resides in the Mobile Cloud and the students can access the data by gaining access to the Cloud by using their mobile devices. This enhances ease of access and convenience as the student can access the education resources from anywhere and anytime.

However, Mobile Cloud Computing has several drawbacks; security is being considered as a major challenge among them. The fact that, any Mobile device can access the institute data opens up a major security risk. To cope with this situation the institute has to seriously think about the data and information security issues. Thus it becomes necessary for the companies and researchers to investigate different data and information security mechanisms.

The authentication of the user who wishes to access the data in the cloud is one of the major security issues that have to be addressed. To make sure that a legitimate user can only access the data in the cloud, a usable, secure and strong authentication mechanism has to be invented.

This paper starts with discussing Mobile Cloud Computing, its benefits and issues. The section 3 discusses various security issues involved in the Mobile Cloud. Section 4 explores the concept of user authentication and various authentication methods proposed for the Mobile Cloud implementation. Section 5 proposes a new secure authentication method based on touch stroke dynamics for the Mobile Cloud.

MOBILE CLOUD COMPUTING

Mobile Cloud Computing refers to an infrastructure where data storage and processing happens outside the mobile device and actually in the cloud [3]. According ABI Research [4] there will be about 1 billion users will be accessing Mobile Cloud and more than 240 million businesses will be using cloud services through mobile devices by 2015. Now users need not spend a lot of money on hardware infrastructure and software, instead they can access it on the cloud.

The Mobile Cloud Computing Forum defines Mobile Cloud as follows [5]: 'Mobile cloud computing is an infrastructure in which both the data processing and data storage are performed outside the mobile equipment. It moves the computing and data storage away from mobile phones and into the cloud, bringing applications to not just Smartphone users but a much broader range of mobile subscribers.

Today, the technology associated with the Smart phones are growing at rapid phase, resulting in more sophisticated Smart mobile devices whose capability can be compared with the personal computers[6]. The modern Smart phones are equipped with a lot of features and applications. They have the capability of being used moving anywhere and accessing the data any time. With their ability of accessing the web anytime and anywhere, the mobile phones can be readily connected to the cloud emerging in a new computing paradigm called Mobile Cloud Computing. Thus Mobile cloud computing is a highly promising technology for the future of mobile computing.

Today a mobile user may require a number of services keeping the mobility factor intact. Mobile Cloud is very well suited for these users who wish to avail these services while moving using their mobile devices. Mobile Cloud can be used for mobile transactions, learning new things and even for listening music anytime and anywhere. As mentioned in the ABI research [7] and Khan et al. [8], Mobile Cloud Computing is being used in a wide range of applications in almost every field of day to day life. The applications of Mobile Cloud

include Email, Mobile Learning, Mobile Commerce, Mobile Gaming and Mobile healthcare.

Mobile Cloud Benefits

In 2011, Zhang et.al [9] developed a framework for collaboration of two technologies namely, Cloud computing and Mobile computing. The idea of accessing the cloud resources over the mobile device has proved to be a remarkable innovative idea that has gained immense popularity due to the convenience and benefits offered by this new technology. As mentioned by Dinh et.al. [10], common Benefits of Mobile Cloud include:

- Limited hardware: The main benefit of Mobile Cloud is that the user need not have sophisticated hardware devices like PC and laptops instead use their Mobile devices to access the cloud.
- Limited battery: Since computations take place in the cloud, battery of the mobile device will be saved.
- Improved storage: Since data gets stored in the cloud, we can store as much data as needed which is not limited by the storage capacity of the mobile device.
- Improved reliability: Another benefit of storing data in the cloud is the fear of data loss is eliminated as the data gets stored in multiple computers.
- Cost reduction: Since cloud supports on demand policy, user can use the cloud according to his requirement and capacity, cost incurred in downloading and installing the applications is reduced.

Mobile Cloud Challenges

As any other new technology, Mobile Cloud Computing has also a number of issues and challenges. Mobile Cloud is the result of the establishment of a bond between two different technologies named Mobile computing and Cloud. Among them, the cloud has maximum computing facilities whereas the mobile device's computing ability is limited. Hence there are a number of issues which are to be resolved with respect to Mobile Cloud. These challenges are related to security, resources and network. Fernando et.al [11] has elaborated the challenges faced by Mobile Cloud. These challenges include:

- Battery and hardware limitations: The battery capacity and computing resources of the mobile device are usually less compared to laptops, in order to keep their cost minimum.
- Availability: Another barrier in the implementation of Mobile Cloud is the availability of internet connection. Low signal reception from the tower might result in frequent disconnections which may result in inefficient operation.
- Bandwidth and latency: mobile devices need to have high bandwidth and low latency, which is difficult to achieve due to network connection problems.
- Security: In Mobile Cloud the user data will reside in the cloud. This may result in many data security issues like integrity, confidentiality and availability of data. Security of data in the cloud is an important research area for the future, since security of data is an important factor in the success of Mobile Cloud.

SECURITY IN MOBILE CLOUD

Mobile Cloud Computing exposes the user's data to a number of security risks. Mobile user's data integrity and privacy are the most important security concerns in the Mobile Cloud. NIST special publication on Guidelines on Security and Privacy in Cloud Computing [12] has provided clear directions on the security and privacy issues faced by the Mobile Cloud. It presented several recommendations for secure implementation of the Cloud. The document gives a brief coverage on threats, risks and probable solutions for the implementation of secure cloud.

In his thesis Sachdeva [13] has studied the possible security challenges faced by Cloud Computing and has coined some directions to solve some of these security issues.

As the name Mobile Cloud implies it is a combination of two different technologies namely, Mobile Computing and Cloud Computing, we have to consider the security risks involved in both these technologies [14]. Thus the security related issues and challenges in Mobile Cloud are divided in to two categories: Mobile Clod User's security; and Mobile Cloud data security as suggested by Huang et al. [15] and Caytiles et al. [16].

Mobile Cloud User Security

These issues are related to the mobile user who uses the facilities offered by the cloud. We know that mobile devices are exposed to different types of security vulnerabilities and risks such as malwares and malicious codes [17], since the mobile device is connected to internet. The connection to the cloud also exposes the mobile device into the cloud causing some privacy issues [18]. Different security concerns related to user security fall into one of the following issues.

Mobile device security: When the mobile device gets connected to the internet, it will be exposed to different types of attacks such as Virus, Malware and malicious code. Thus getting connected to the cloud implies exposing the mobile device into different security attacks. Installing antivirus programs might be a solution, however, practically it is a constraint on a mobile device. Hence the Mobile Cloud should provide some solution to this problem.

Privacy of the User: When user connects to the cloud through internet, all the private information related to the user such as user's present location is exposed. Revealing of such private information related to the user is undesired by the user and hence some solution has to be found for this problem.

Data Security and Access: Generally the cloud hosts certain user data such as contact information, calendar of events and personal data files. This remote data storage results in exposure of personal information in to the cloud and can be misused by unauthorized person. Another issue in this remote storage is availability of data whenever desired. Secure data storage and anytime availability of user's data is an important security concern in the implementation of Mobile Cloud. Hence proper measures are required to make the remote data secured and always available.

Mobile Cloud Data Security

Modern industries and individual users have started to take advantage of large storage space provided by the Mobile Cloud

by storing their data and personal files in the cloud. However, a number of security issues arise when the user's data resides in the cloud. These include Data Ownership, Data Integrity, Authorization and Authentication.

Data Ownership: Since the user's data resides in the cloud, any other person can download it and use it for illegal purpose. This leads to piracy of digital content such as video, image and textbooks and results in ambiguity in ownership of the downloaded data. Mobile cloud provides scope for such illegal usage of user's data and is an important security concern. To provide solution for this problem cloud has to implement certain encryption and decryption techniques, so that only authorized users can use the data.

Data Integrity: Data integrity deals with correctness and completeness of data. If the data is stored personally one can be sure of data integrity. However when user stores his data remotely in the Mobile Cloud, there will be some doubts about the completeness of data. Damage to the user data can occur in the cloud, since cloud does not have proper integrity control mechanisms. Hence for successful Mobile Cloud implementation, suitable integrity control measures have to be taken by the cloud provider in order to ensure user's data integrity.

Authentication: Authentication is a process in which one entity verifies and confirms the legitimacy of another entity. The authentication can be achieved in many ways; using something that user knows such as user name and password, using something that user has such as Personal Identification Number (PIN) or using something that user inherently is such as finger print of the user. For providing strong security, the Mobile Cloud should have proper as well as a strong authentication mechanism to make sure that illegal user does not enter into the system.

Authorization: Authorization is the process in which the system makes sure that the user has proper right to certain resources. Generally each valid user will be given certain access rights to certain resources. For example a valid user after authentication process can withdraw money from ATM machine. However he is authorized only to withdraw money which is within a maximum amount fixed by the bank. For providing strong security, the Mobile Cloud should have proper authentication mechanisms to make sure that illegal users can not access restricted resources.

Thus data security is the major security concern of the companies that are willing to adapt Mobile Cloud. Many of these security issues arise due to the fact that the company does not have any control over the data stored in the cloud. Web browsers and Web services add up the security concern in the cloud since the cloud is accessed through the internet. Proper security mechanisms have to be developed for the cloud computing environment to secure the data that can be accessed through the mobile devices [19].

AUTHENTICATION IN MOBILE CLOUD

All authentication methods require the user to specify who he is or what he knows or what he has to prove that he is the legitimate user of that system. What user knows refers to the password; what user has refers to the Smartcard and what user is refers to biometrics such as the fingerprint of the user. Generally, selection of proper authentication mechanism for a particular system is based on the device being used by the user and trust level of the system.

Modern mobile devices offer greater flexibility in installing different types of applications to be used in a variety of purposes. People nowadays use their mobile devices for versatile uses such as keeping track of their meetings, to store images and videos, to access internet, email and also to access the cloud. A number of sensitive personal information is being stored in mobile devices. Thus modern smart phones have been considered by users as the lighter versions of computers.

However, modern smart phone's ability to act as always-on devices makes them an easy to attack devices. The data stored in these devices are at risk of different types of security attacks, when these devices are connected to the cloud. In addition, mobile devices can be easily lost or stolen and the intruder third party can access the confidential data that is being stored in the cloud. Hence it is necessary to have a strong and secure authentication scheme for mobile devices accessing the cloud. A number of authors have proposed some authentication mechanisms for the Mobile Cloud environment which are discussed below.

Chow et.al [20] has proposed an authentication framework based on behavioral authentication, translating user behavior into a score. Score is assigned to the users on the basis of observed behavior and it is processed using some statistical method. The user is authenticated only if the score lies within a threshold value. The method performed well for small number of users. However as the number of users increase, the performance started to degrade since the authentication is performed by the third party.

Xiao et.al [21] has proposed a lightweight authentication scheme based on dynamic credentials. The method is based on the communication between the mobile network and the cloud service provider. During registration phase some dynamic secrets are shared by the cloud service provider and the user. If same dynamic credentials are given by the user he will be authenticated. However, if user forgets the secrets shared by him during registration, he will be found adversary and authentication is denied.

An authentication scheme for Mobile Cloud using Subscriber Identity Module (SIM) was proposed by Z. Ahmed et.al [22]. The authentication was done during boot time which was based on Universal SIM. The authentication was achieved based on the response received from the user for a unique random challenge. The scheme showed good performance. However this scheme works only if the mobile device supports the Universal SIM and does not support other devices such as tablets and laptops.

In 2011, Oh et.al [23] has proposed an authentication scheme based on Quick Response Code (QR Code). In this scheme, user is supposed to enter user id and password. Along with that the user's image was to be captured by the mobile device. Then all these three; user id, password and image will be converted into a QR Code. Based on the code received authentication is achieved. The scheme provided good authentication since it uses the valid user's image. However it resulted in additional burden on the Smart phone user to capture the image and send it to the Cloud server.

In 2012, Yoo et.al [24] has proposed a multiuser authentication scheme for the cloud environment based on Cellular Automata.

It was a lightweight scheme for authentication in the Mobile Cloud. The authentication is based on the communication between the mobile network and the cloud server. The mobile network performs the authentication and then sends it to the cloud. The scheme used the mobile network as the third party for authentication.

Omri et.al [25] has proposed an authentication scheme for the Mobile Cloud environment by using the handwriting recognition. The mobile device acts as a biometric capturing device for capturing the handwriting of the user. Since the handwriting of a user is usually unique, this scheme proved to be good scheme for authentication. However it gives additional burden on the user to capture the handwriting and then send it to the cloud server.

Park et.al [26] has proposed an authentication mechanism based on SSP-M Cloud protocol. The scheme had two phases: Smart phone verification and Cloud verification. In this the authentication is done in the SSP-M Cloud environment based on user id and password. Additional authentication was not included in this scheme.

Authentication in the Mobile Cloud environment using the concept of profiling was introduced by Jeong et.al [27]. The user profile had two parts: User information and Service information. User information includes user name, user ID and some personal information such as hobby. Service information includes Service name, service provider and context of the service. Using these user and service information an user profile was created, which is used for authentication of the legitimate user. This was a form of behavioral biometric authentication. Performance of this scheme was good however; it requires complex processing to create the user profile and authentication.

Authentication in the Mobile Cloud using the concept of Message Digest was proposed by Dey et.al [28]. In this scheme, an encrypted hashed message was used for authentication of the user. The scheme included both registration and authentication. The scheme was complex in processing since it included both encryption and hashing.

In 2013, Chen et.al [29] has proposed an authentication scheme using the familiar one-time password. In this scheme, a Generic Authentication Architecture was built in the mobile device which supports the Universal SIM. The user provides the user id and password to the server and the server provides a one-time password to the user for authentication. The scheme resulted in delay in authentication as the user has to wait for the one-time password. Also the scheme was applicable to mobile devices which had USIM.

IehabALRassan et.al [30] has proposed an authentication scheme for the Mobile Cloud using Fingerprint. Along with the user id and password, the user has to provide the image of his fingerprint to the cloud server. The cloud server authenticates the user after verifying the user credentials and the fingerprint. The scheme's performance was good for authentication purpose since the fingerprint of each user is unique. However it resulted in additional burden for the user to send the fingerprint to the server and resulted in delay in processing.

Momeni [31] has proposed a lightweight authentication scheme for the Mobile Cloud using the mobile network. The method employed a local authentication in the mobile network using user id and password. After authenticating the user the information is communicated to the cloud server. It included a registration phase and mutual authentication using session key agreements. This scheme had used the mobile network of the user as the third party for authentication.

AUTHENTICATION USING TOUCH STROKE

From the Literature study, we found that a number of authentication methods have been proposed. These methods are complex in nature with respect to Smart phone user convenience. When authentication of user has to be done who uses the smart phone, user convenience has to be given greater importance. Hence it becomes necessary to develop a simple novel authentication mechanism that considers both user convenience and security in mind.

We have introduced the concept of touch stroke dynamics in the authentication process. It is a type of authentication in which the touch speed of the user is used for authentication.

The proposed system includes two systems, one is the cloud server that is used to store the documents uploaded by the teachers and the other one is the client mobile. The client will connect to the server in order to access the learning materials. The server will authenticate the user and only valid user is allowed to access the materials.

The user is required to install the learning app on their mobiles and register with a valid username and password. During registration the touch duration of username and password are also get stored in the server.

During Authentication phase, when user types his username and password the touch stroke length is measured by the server and authentication is granted only if both password and touch stroke length are matched.

Two versions of learning apps were developed in order to compare the performance of the authentication schemes. One version uses the simple password authentication and the second version uses the touch stroke length authentication method. Both applications were installed on the same android phone and tested with different username and passwords.

A total of 50 username and passwords having different levels of complexities were tested on the two applications and the total time required to authenticate the user using each application were measured. The results were plotted on the graphs which are shown below.

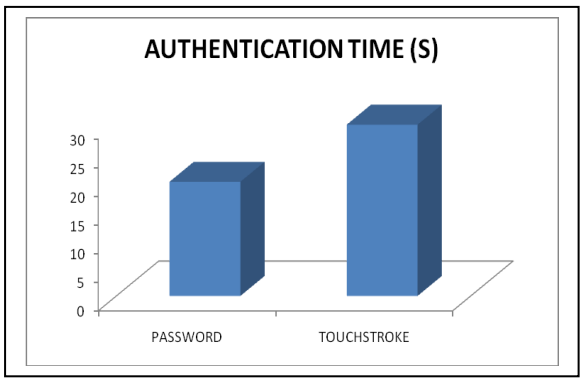

Figure 1. Authentication using simple passwords

When simple passwords were used by the users, the average authentication time is found to be 14 seconds for password method and 24 seconds for touchstroke method.

When complex passwords were used by the users, the average authentication time is found to be 20 seconds for password method and 30 seconds for touchstroke method.

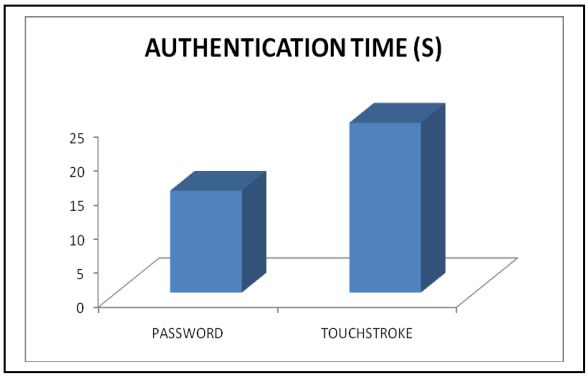

Figure 2. Authentication using complex passwords

From the test results it is clear that the use of the enhanced authentication method called touch stroke length authentication does not have much impact on the total time required to authenticate the user. The total time difference between the two methods is very nominal and negligible.

At the same time the touch stroke length method validates both password and touch stroke length and provides a form of two stroke authentication which provides enhanced security. Thus it is evident that the proposed method provides additional security without compromising on user convenience.

During these experiments a parameter Δ is used which is the liberty time for touch stroke authentication. It is time difference between the original touch stroke length stored in the server and the touch stroke length during login.

The parameter is required only to provide time flexibility and relaxation for the user during login. The method can be made further strict and more secure by reducing the liberty time during authentication.

CONCLUSION

Mobile Cloud Computing is one of the latest trends in the information technology sector, which combines the advantages of both mobile computing and cloud computing. It provides greater flexibility for the user to access the cloud resources. At the same time the Mobile Cloud faces several security threats which have to be dealt with greatest care. Continued research has to be done in order to identify latest threats and generating an action plan to tackle such threats. One of the major concerns to face the security threats is to authenticate the legitimate user of the system. From the literature study, several authentication schemes have been developed in the recent past. However, keeping in mind the convenience of the Smart phone user, it becomes necessary to develop a smarter authentication scheme that combines both user convenience and stronger security. We have proposed a simple authentication method which is fairly secure that establishes a balancing act between security and convenience of the smart phone user in the Mobile Cloud environment.

REFERENCES

[1] Miller, Keith W., Jeffrey Voas, and George F. Hurlburt, "BYOD: security and privacy considerations," *IT Professional*, vol. 14, issue 5, pp. 53-55, 2012.

[2] Xiaopeng Fan, Jiannong Cao, and Haixia Mao. "A Survey of Mobile Cloud Computing," ZTE Communications, vol. 9, No. 1, pp. 4-8, March 2011.

[3] Han Qi, Abdullah Gani, "Research on Mobile Cloud Computing: Review, Trend and Perspectives," *Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP)*, Bangkok, pp. 195 – 202, 2012.

[4] ABI, "Mobile cloud computing subscribers to total nearly one billion by 2014," http://www.abiresearch.com/press/1484/, Tech. Rep., 2009.

[5] Mobile Cloud Computing Forum, Available: http://www.mobilecloudcomputingforum.com

[6] Li, Xun, et al. "Smartphone evolution and reuse: Establishing a more sustainable model." *39th International Conference on Parallel Processing Workshops (ICPPW), IEEE*, 2010.

[7] ABI, "Mobile cloud applications," Available: http://www.abiresearch.com/research/1003385

[8] A.U.R. Khan, M. Othman, S.A. Madani, and S.U. Khan, "A Survey of mobile cloud computing application models," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 393-413, 2014.

[9] X. W. Zhang, A. Kunjithapatham, S. Jeong, and S. Gibbs, "Towards an elastic application model for augmenting the computing capabilities of mobile devices with cloud computing," *Mobile Networks & Applications*, vol. 16, no. 3, pp. 270–284, 2011.

[10] Hoang T. Dinh, Chonho Lee, Dusit Niyato, Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless Communications and Mobile Computing,* Wiley, 2011.

[11] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, no. 1, pp. 84–106, January 2013.

[12] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing", NIST Special Publication 800-144, Available: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494.

[13] K, Sachdeva, "Cloud Computing: Security Risk Analysis and Recommendations," Master Thesis, University of Texas, Austin, 2011.

[14] Le Guan, Xu Ke, Meina Song, and Junde Song, "A Survey of research on mobile cloud computing," *IEEE/ACIS 10th International Conference on Computer and Information Science (ICIS)*, pp. 387-392, 2010.

[15] D. Huang, Z. Zhou, L. Xu, T. Xing And Y. Zhong, "Secure data processing framework for mobile cloud computing", *IEEE Infocom 2011 Workshop On Cloud Computing,* IEEE, pp. 620-624, 2011.

[16] R. D. Caytiles, S. Lee, "Security considerations for public mobile cloud computing," *International Journal of Advanced Science and Technology*,Vol. 44, pp 81-89, July, 2012.

[17] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, "Towards secure mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, Issue 5, pp 1278-1299, July 2013.

[18] S. Abolfazli, Z. Sanaei, and A. Gani, "Mobile cloud computing: A review on smartphone augmentation approaches," in *Proc. 1st Inernational Conference on Computing, Information Systems, and Communications (CISCO12)*, Singapore, May 2012.

[19] Altinkemer, K. and T. Wang, "Cost and benefit analysis of authentication systems," *Decision Support Systems*, vol. 51, pp. 394-404, 2011.

[20] 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 Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW)*, pp. 1 - 6, 2010.

[21] Xiao, W. Gong, Mobility can help: protect user identity with dynamic credential, *in Proc. 11th Int. Conference on Mobile Data Management, MDM "10, Missouri, USA*, May 2010.

[22] Z. Ahmad, K. E. Mayes, S. Dong, and K. Markantonakis, "Considerations for mobile authentication in the Cloud," *Information Security Technical Report*, vol. 16, no. 3-4, pp. 123–130, Aug. 2011.

[23] D. S. Oh, B. H. Kim, and J. K. Lee, "A Study on authentication system Using QR code for mobile cloud computing environment," *Future Information Technology*, pp. 500-507, 2011.

[24] K.-Y. Yoo, "A lightweight multi-user authentication scheme based on cellular automata in cloud environment," *2012 IEEE 1st International Conference on Cloud Networking (CLOUDNET)*, vol. 1, no. 1, pp. 176–178, Nov. 2012.

[25] F. Omri, R. Hamila, S. Foufou, and M. Jarraya, "Cloud-ready biometric system for mobile security access," *Networked Digital Technologies*, pp. 192-200, 2012.

[26] JiSoo Park, Ki Jung Yi and Jong Hyuk Park, "SSP-MCloud: a study on security service protocol for smartphone centric mobile cloud computing", Journal of IT Convergence and Services, Springer, 2012.

[27] Hoon Jeong, Euiin Choi, "User authentication using profiling in mobile cloud computing, *AASRI Procedia*, vol. 2, pp. 262–267, 2012.

[28] Saurabh Dey, Srinivas Sampalli, Qiang Ye, " Message digest an authentication entity for mobile cloud computing," *IEEE 32nd International Performance Computing and Communications Conference,* pp. 1-6, 2013.

[29] Chunhua Chen, Chris J. Mitchell and Shaohua Tang, "Ubiquitous one-time password service using the generic authentication architecture", *International Journal of Mobile Networking Applications*, Springer, pp. 738-747, 2013.

[30] IehabALRassan, HananAlShaher, "Securing mobile cloud using finger print authentication," *International Journal of Network Security & Its Applications*, Vol.5, No.6, November 2013.

[31] Mohammad Rasoul Momeni, "A lightweight authentication scheme for mobile cloud computing," *International Journal of Computer Science and Business Informatics,* vol. 14 no.2, pp 153-160, August 2014.