Volume 1, No 3, August 2015 **ISSN: 2348 4454**
International Journal of Emerging Trends in Computing and Communication Technology
Available @ www.ijetcct.in

A Survey on User Authentication Mechanism in Mobile Cloud Computing

A. Cecil Donald[1], M. Regin[2], Dr. A. Aloysius[3], Dr. L. Arockiam[4]

[1]*Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli*
[2]*M.Phil Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli*
[3]*Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli*
[4]*Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli*

ABSTRACT

Cloud Computing is an emerging technology which is widely used in various applications all over the world. Security is always a major consideration as it holds the sensitive data. It is essential to authenticate the users to provide an authorized access to their data. In Mobile Cloud Computing (MCC), a lot of studies are being carried out to exterminate the issues to make cloud service more reliable and secure because more sensitive data are stored in the Mobile Cloud Environment (MCE). This paper elucidates various authentication mechanisms proposed by various researchers in the area of Mobile Cloud. An analytical survey is also carried out in this paper to identify the problems and issues present in the existing mechanisms.

Keywords

Mobile Cloud Computing (MCC), Security, Authentication, Key Generation, Identification, Denial of Service (DoS).

1. INTRODUCTION

Cloud computing is the most demanding and emerging technology throughout the world. Combination of Mobile Computing and Cloud Computing is called Mobile Cloud Computing (MCC). MCC is defined as "a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the Internet". According to International Data Corporation (IDC) [1], "Mobile Cloud Computing is a new platform combining the mobile devices and cloud computing to create a new infrastructure, whereby cloud performs the heavy lifting of computing-intensive tasks and storing massive amounts of data". Best example for cloud service Amazon EC2, Google Apps, etc. Data security has many aspects like Authentication, Confidentiality, Integrity, and Availability. There is a need to improve the mobile cloud security by strengthening the authentication system [2]. Authentication is the key of security services including confidentiality and integrity [3]. Authentication is the process of verifying the user's identity in order to have authorized access to their data. Using Authentication parameters, user's sensitive data can be protected from internal and external attack. This paper mainly discusses on the existing authentication mechanisms and their issues.

2. RELATED WORKS

Francisco Corella et al. [4] proposed one, two and three factor authentication methods that can be used for mobile devices. This method provides strong security and also, it provides more suitable to use One Time Passwords (OTPs) or ordinary passwords. The proposed authentication methods simply use Public Key cryptography. The advantage of this scheme is easy to implement and deploy, because all cryptography is condensed in black boxes. So, there is no need to program any cryptographic operations by developers and easy to deploy. They do not require Public Key Infrastructure (PKI) and avoid the use of digital certificates.

Yogesh Patel et al. [5] have proposed Multilevel Authentication. The proposed mechanism aims to enhance authorization and authentication process by using multilevel authentication. It is used to protect cloud from malicious user and unauthorized access. This scheme implements security measure to protect data of users which is stored in cloud environment. It also provides service level security. Here, user based access control is applied over user's data. (i.e.) User can grant, revoke sharing permission at any point.

Yeh et al. [6] proposed a mobile authentication system. This system has some features including One Time Password, Completely Automated Public Turing Test (CAPTT) to tell computers and humans apart, Voice identification of creatural features, and visual cryptography, designing a formula where users are not required to remember any accounts/passwords when they use the internet through mobile devices. It aims at smart phones and the Cloud. The main thing is to improve the problems of Internet fishing and the management of passwords. This research includes phases of registration and login. It not only increases user's convenience and security but also prevent the internet from key log and fishing attack.

Iehab Al Rassan et al. [7] have proposed and implemented a user authentication mechanism using fingerprint recognition system for Mobile Cloud. Fingerprint

images of users are captured with the use of mobile phone camera and processed to access mobile cloud resources. The proposed scheme is implemented to show that the security is enhanced with accepted performance level in Mobile Cloud. The proposed solution is not only to secure unauthorized access, but also for database protection from injection attacks due to the absence of string input from users.

Vineet Guha et al. [8] have described review of certain security concerns in cloud computing technology and also about certain ways to restrict and overcome such issues over SaaS & PaaS Layers using mobile technologies. In this scheme, user is allowed to keep its information publicly accessible to all or either secured or restricted that is accessible only by providing legal key. Once this key is provided to the service provider, it actually authenticates the key along with the network from where the request has been made and this validation is called as "Digital Confirmation". If such information is authenticated and user is found to be authorized user and are able to see download and make changes to it, the information else invalid and information is thrown to the user.

Indrajit Das et al. [9] have proposed a user registration and authentication method. Both the methods are secure and easy to use by fulfilling the needs of cloud service authentication. These methods use a mobile device to generate one time passwords in cloud services. To use the AES encryption, the client and the server have been configured and communicated. Their proposed scheme provided good security and easy to use for clients.

Mohammad et al. [10] suggested a lightweight authentication protocol for mobile cloud environment. The major advantages of this mechanism is, it supports local authentication, user anonymity and also resistance against attacks such as modification attack, replay attack, server spoofing attack, stolen verifier attack and so on. Mobile user is authenticated in his/her mobile network. This mechanism saves bandwidth, provides low latency.

Jin et al. [11] proposed two systems namely user authentication and mobile device authentication system with hybrid cloud service server. In their research, the proposed systems tend to support device certification, user authorization and service authentication certificate to the user in an easy manner. It uses two factor authentication and RADIUS method schemes. So, a secure authentication system is proposed for the hybrid cloud service in Mobile Cloud Environment and also, their mechanism is able to provide security, applicability, availability and resistance against Man-in-the-Middle attack. User authorization device certification and service authentication is supported by proposed scheme. Complement security services can't be provided by the RADIUS server.

Davit [12] discussed the Authentication and Authorization System in Cloud Environment. In this paper, the author proposed cloud security system and contributions are made in the area of authentication and authorization. Author proposed the architecture which consists of central and portal security servers. It has the advantages of flexible, secure, reliable and effective and it is easy to manage. There is no privacy in this process. All security credential are stored in central security system. So, end user activities are traced by cloud identity service provider.

Chow et al. [13] discussed the framework and applications in mobile cloud. In this research, authors refer users past behavioral data for authentication. They have proposed a cloud authentication system. It has a core authentication service that is trust cube which resides in the cloud. The proposed system has the tendency to accept various authentication methods.

Gokaj et al. [14] presented an authentication mechanism, by using different technologies like Mobile Signature, SSL, SOA, SFTP and combine them to provide a complete solution for a mobile cloud environment. By the Mobile Signature the user identity is assured. This is an easy way to track the real person of each operation. By using SSL in the middle, the communication channel is secured. The session key and the sequence number make it impossible for a Man-in-The-Middle to replace or retry the network message.

Deepa et al. [15] discussed different types of authentication methods such as password and PIN based Authentication, SMS based Authentication, Symmetric key, public key Authentication, and Biometric Authentication. They have proposed multi factor Authentication. It is more complicated for an unauthorized access. User Anonymity and Availability are not addressed. It is more secure but using biometric is more cost efficient.

Sanjoli et al. [16] discussed Authentication in cloud security. In this work, they have used the Rijndael encryption algorithm along with EAP-CHAP encryption algorithm for Authentication. EAP-CHAP algorithm is used to solve the authentication and Authorization problems in cloud computing. Rijndael algorithm is most secured Algorithm. They have mainly focused on the client side security. Both encryption and decryption are done by the user so that, intruder can't decrypt the data.

Cecil et al. [17] discussed different security issues in Mobile Cloud authentication and Identity Management and the way it works. They also discussed security issues and corresponding approaches of Mobile Cloud Computing. Further, the strengths and weaknesses of user authentication techniques were also discussed.

Kashif et al. [18] proposed a cloud security model and framework for Authentication. It provided convenient and secure connection to the user for accessing cloud. They used SSO Technology. Because of this technology user can access multiple services. They said about RBAC policy. This policy provides simplicity and flexibility for capturing Dynamic requirements.

Neha et al. [19] designed cloud architecture which is secure at client and server end, they have used Elliptic Curve cryptography for data encryption and Diffie-Hellman Key Exchange mechanism for connection establishment. But the complexity of Cryptographic algorithm directly affects the speed of access. They have used Elliptic Curve Cryptography (ECC) as computation cost and speed of algorithm is less. It has a sub exponential, time complexity because it is difficult to crack.

3. MOTIVATION

MCC is based on both mobile and cloud computing. Mobile Cloud Computing has various challenges and issues especially, security. In security, Authentication is the foremost issue as it is the doorstep for accessing cloud services. Authentication process helps to prevent user's data from third parties. The following section makes a critical analysis on various authentication mechanisms proposed for Mobile Cloud Environment.

4. COMPARATIVE ANALYSIS

From the broad literature review of existing and proposed authentication mechanisms in Mobile Cloud explained in section 2, a critical comparative analysis is made which is shown in table 1 that lists out the advantages and disadvantages of those mechanisms.

Table 1 Comparative Analysis of various Authentication Mechanisms

Author	Existing Mechanisms	Advantages	Drawbacks / Limitations
Francisco et al.	One- two- and three factor authentication Mechanism	Provides Strong security, Easy to use	Not suitable for all environments
Yogesh Patel et al.	Multilevel Authentication	Provides service level security and provides User Based Access Control	User needs to enter credentials every session
Yeh et al.	Visual Password Authentication Scheme	No need to remember any passwords	Variability in the voiceprint characteristics, Information Loss
Rassan et al.	Fingerprint Authentication Mechanism	Improved Performance and Security	No input is allowed from user to enter the system
Vineet Guha et al.	Key Generation Mechanism	Network Key, Suits SaaS & PaaS	Inaccurate results
Indrajit Das et al.	Authentication Mechanism	Easy and light weight	Not Secure and time Delay
Mohammad et al.	Lightweight Authentication Protocol	Easy authentication, Reduces Latency	Consumes more time especially in wireless communications.
Jin et al.	Mobile Device authentication	Supports authorization service, device certification	RADIUS server can't provide security services
Davit	Authentication and Authorization techniques	Flexible, security, reliable and effective	No Privacy
Chow et al.	Behavioral Authentication	Trust Cube Method	Not Supported for all devices
Gokaj et al.	Mobile Signature Authentication	Lightweight Mechanism	Unable to detect the attacks
Deepa et al.	Multifactor authentication using smart phones as software tokens.	No external Devices and generates unique One Time Passwords (OTP)	User Anonymity and Availability is not addressed
Sanjoli et al.	Rijndael encryption with EAP-CHAP encryption	Provides Authentication and Authorization	Prone Server Port attack
Kashif et al.	SSO based authentication	Ability to access Multiple Services	Prone to man-in-the Middle Attack
Neha et al.	Data encryption and Key Exchange mechanism	Secure Connection	Time delay due to Complexity

5. ISSUES AND CHALLENGES IDENTIFIED

From the broad literature review of existing and proposed authentication mechanisms in Mobile Cloud explained in the above section, it is evident that there are some major issues and challenges in MCC. Those issues and challenges are highlighted and categorized below. The security related issues are then divided into two broad categories as listed below.

a. Mobile Cloud Infrastructure Issues
b. Mobile Cloud Communication Channel Issues

5.1 Mobile Cloud Infrastructure Issues

From the cloud infrastructure point of view, a variety of attacks are possible on the cloud. Some of these attacks are given below.

- Attacks on Virtual Machines
- Authorization and Authentication
- Attacks from Local Users

5.2 Mobile Cloud Communication Channel Issues

A lot of improvement needs to be done in the mobile cloud communication channel. The following attacks exist on communication channel.

- Access Control Attacks
- Attacks on Authentication
- Attacks on Availability
- Data Integrity Attacks

Some of the mobile communication channel related issues are pointed out below.

- Low Bandwidth and Latency problems
- Availability of desired services
- Heterogeneity
- Limited Resources

5.3 Other Issues and Challenges

Even though there are several advantages, the MCC possesses some limitation which in turn affects the usage of cloud services. They are,

- Resource Poverty Mobile Devices
- Network Bandwidth
- Security and Privacy
- Latency
- Heterogeneity
- Computing Offloading
- Data Accessibility
- Data Ownership

5.4 Threats in MCC

a) Loss of Data

Cloud Security Alliance (CSA) says that the data stored in the cloud can be stolen by intruders/hackers. Data can suffer a natural disaster or data can be accidentally deleted if a provider of cloud services does not host proper backup methods. On the other hand, the user who encrypts his/her data before uploading them into the cloud may lose the encryption key.

b) Service Traffic Hijacking

In the cloud environment, attacker could use the stolen login credential to capture or give distorted information or forge to redirect users to malicious sites. Organizations should not allow the distribution of their login information for all services. CSA also recommends secure, strong two factor authentication to reduce the risks.

c) Denial of Service

The cloud can be attacked using Denial of Service (DoS) that causes an overload to the organization, making use of a huge amount of system resources and not allowing users to use the desired service. Media attention often involves DoS attacks which can block the cloud usage. For example, attackers can launch DoS attacks on asymmetric application layer by using vulnerabilities in the web servers, cloud resources or other databases to fill up the application with a payload.

d) Malicious Insiders

Without a proper level of security on SaaS and PaaS, an insider who has improper targets may gain access to the confidential data. Malicious insiders are certified to do bigger and greater damage than any other attacks on resources. According to CSA, the system is vulnerable to attacks if the keys are not kept with the customer even if encryption is applied on the data.

e) Data Theft

The biggest risk in IT is the theft of confidential corporate information, but CSA indicates that the cloud model offers a new technology and at the same time it holds the pool of attacks. If the base of the cloud data from multiple leases is not understood properly, that flaw in the application of one client can attack and affect the data of the other cloud users.

6. CONCLUSION

Mobile cloud computing is a rich computing technology and a profitable field of business people because it reduces the running and development costs of Mobile Cloud Environment. Security is the top most issue and it needs to be resolved. Only authorized access to their data becomes vital important in the mobile cloud. This paper analyzed various existing authentication mechanisms and identified the problems that need to be resolved. From this study, it is essential to develop a user authentication mechanism that is not only secure but also should be lightweight and cost efficient.

7. REFERENCES

[1] http://www.cse.wust.edu/~iain/cse 574=10/ftp/cloud/index.html

[2] B. H. Kim, D. S. Oh, and J. K. Lee, "A Study on Authentication System Using QR Code for Mobile Cloud Computing Environment", Future Information Technology, 2011, pp. 500-507.

[3] Paramvir Bahl, Richard Y. Han, Li Erran Li, Mahadev Satyanarayanan, “Advancing the State of Mobile Cloud Computing”, Microsoft Research, UK, ACM, June 25, 2012, 978-1-4503-1319-3/12/06, pp.58-64.

[4] Francisco Corella, Karen lewison, “Strong and Convenient Multi-Factor Authentication on Mobile Devices”, Vol. 2, Issue 7, September 6, 2012, pp. 12-18.

[5] Yogesh patel, Nidhi sethi, "Enhancing Security in Cloud Computing using Multilevel Authentication", International Journal of Electrical and Electronics & computer Science Engineering, Vol. 1, Issue 1, February 2014, ISSN: 2348-2273, pp. 320-325.

[6] Her Tyan Yeh, Bing chang chen, Yi-cong wu, "Mobile user Authentication System in Cloud Environment", International Journal of Security and Communication Networks, November 2012, pp. 74-79.

[7] Iehab AL Rassan, Hanan Al Shaher, "Securing Mobile cloud Using Finger print Authentication", International Journal of Network security & its applications (IJNSA), Vol. 5, No. 6, November 2013, pp.5-9.

[8] Vineet Guha, Manish shrivastava, "Review of Information Authentication in Mobile Cloud Server SaaS & PaaS Layers", International Journal of Advanced Computer Research, Vol. 3, No. 1, Issue 9, March 2013, ISSN: 2249-7277, pp. 31-35.

[9] Indrajit Das, Riya Das, "Mobile Security (OTP) by Cloud Computing", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 2, Issue 4, August 2013, ISSN: 2319-1058, pp. 114-118.

[10] Mahnoush Babau Zadeh, Majit Bhaktiari, Mohol Aizaini Maar, "Keystroke Dynamic Authentication in Mobile Cloud Computing", International Journal of Computer Applications, Vol. 90, No.1, March 2014, ISSN: 0975-8887, pp. 35-39.

[11] Jin mookkim, Jeong-Kyung moon, "Secure Authentication System for Hybrid Cloud service in Mobile Communication Environments", International Journal of Distributed Sensor Networks, Vol. 2, July 2014, pp. 62-66.

[12] Davit Hakobyan, "Authentication and Authorization Systems in Cloud Environments, International Journal of Information and Communication Technology, Vol. 4, Issue 5, October 2012, pp. 165-169.

[13] Richard Chaw, Markus Jakobsson, Ryusuke Arasuoka, "Authentication in the Clouds: A Framework and its Application to Mobile Users", CCSW, ACM, October 2012, pp. 352-358.

[14] R. Gokaj, M. Ali Aydin, R, Selami Z bey, "Mobile Cloud Authentication and Secure Communication", In Proc. of International Conference on Information Security and Cryptology, September 2013, pp. 42-45.

[15] Deepa pause, P. Haritha, "Multi Factor Authentication in Cloud Computing for Data storage Security", International Journal of Advanced Research in Computer Science and Engineering, Vol. 4, Issue 8, August 2014, ISSN: 2277-128X, pp. 14-18.

[16] Sanjoli single, Jasmeet Singh, "Cloud Data Security Using Authentication and Encryption Technique", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), Vol. 2, Issue 7, July 2013, ISSN: 2278-1323, pp. 81-85.

[17] A. Cecil Donald, L. Arockiam, "Securing Data with Authentication in Mobile Cloud Environment: Methods, Models, Issues", International Journal of Computer Applications, Vol. 94, No. 1, May 2014, ISSN: 0975 – 8887, pp. 25-29.

[18] Mashif Munir, Sellappan palaniappan, "Framework for Secure Cloud Computing", International Journal on Cloud Computing: Services and Architecture, Vol. 3, No. 2, April 2013, pp. 95-99.

[19] Neha Tirthani, Ganesan R., "Data Security in Cloud Architecture Based on Diffie-Hellman and Elliptical Curve Cryptography", Vol. 4, Issue 7, July 2013, pp. 82-86.

AUTHOR'S BIOGRAPHY

A. Cecil Donald received his Masters in Software Engineering from Anna University, Chennai, India. He has one year experience in IT industry as a Software Developer. Currently, he is a Ph.D. research scholar in the department of Computer Science, St. Joseph's College, Tiruchirappalli affiliated to Bharathidasan University, India. His main area of research is Mobile Cloud Computing. He has published seven papers in the International Journals with impact factors and presented two research papers in the International Conferences. He has atteneded several national and international conferences and workshops.

M. Regin received her Masters in Computer Science from Bharathidasan University, Tiruchirappalli, India. Currently, she is a M.Phil Scholar in the department of Computer Science, St. Joseph's College, Tiruchirappalli affiliated to Bharathidasan University, India. Her main area of research is Mobile Cloud Computing. She has presented two papers in the National Conference. She has atteneded several national and international conferences and workshops.

Dr. A. Aloysius is working as Assistant Professor in the Department of Computer Science, St. Joseph's College, Tiruchirappalli, Tamil Nadu, India. He has 15 years of experience in teaching and 11 years of experience in research. He has published more than 26 research articles in the International & National Conferences and Journals. He has also presented a research article in the International Conference held at Bali, Indonesia and awarded with the Best Paper. He has delivered invited talks in National and International Conferences.

Dr. L. Arockiam is working as Associate Professor in the Department of Computer Science, St. Joseph's College, Tiruchirappalli, Tamil Nadu, India. He has 26 years of experience in teaching and 18 years of experience in research. He has published more than 226 research articles in the International & National Conferences and Journals. He has also presented 3 research articles in the Software Measurement European Forum in Rome, Bali and Malaysia. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has Co-authored 5 books. His research interests are: Cloud Computing, Big Data, Cognitive Aspects in Programming, Data Mining and Mobile Networks. He has been awarded "Best Research Publications in Science" for 2009, 2010, 2011 & 2015 and ASDF Global "Best Academic Researcher" Award from ASDF, Pondicherry for the academic year 2012-2013 and also the "Best Teacher in College" award for the year 2013 & 2014.