IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Mobile Cloud Computing Authentication: Methods and Techniques with Capabilities, Limitations

Manjusha Anant Shinde Bhandwalkar[1*], Jadhav Shradha Ramesh[2]

[1,2]Dept. of Computer Science & Information Technology Rajarshi Shahu Mahavidyalaya, Latur (Autonomous) Maharashtra, India

Corresponding Author: smanjusha077@gmail.com

Available online at: www.ijcseonline.org

Accepted: 11/Dec/2018, Published: 31/Dec/2018

Abstract:- Today the capabilities of mobile devices have improved real world user friendly applications, storage and feature support. The storage capacity can tremendously be increased with the use of cloud computing. Cloud computing is a flexible, cost effective and proven delivery platform for providing services. Mobile cloud computing means the availability of cloud computing services in a mobile environment. There are various authentication techniques being used like password, log off system, Biometric techniques. This process serves as a protection against different sorts of attacks where the goal is to confirm the identity of a user and the user requests services from cloud servers. Multiple authentication technologies have been put forward so far that confirm user identity before giving the permit to access resources. Authentication in cloud was fully explained in this paper together with the existing methods and the factors with its limitations.

Keywords: cloud computing , mobile cloud computing, authentication techniques

I. INTRODUCTION

The widely use of mobile phone lead to the prosperity of mobile services. Dream of "Information at your fingertips anywhere, anytime" has become true. However, mobile devices still lack in resources compared to a conventional information processing device such as PCs and laptops. Also, the limitation of battery restricts working time. How to augment capability of mobile phone has become the important technical issue for mobile computing. The cloud computing brings opportunities for this demand. Cloud computing provide new supplement, consumption, and delivery model for IT service. Cloud-based services are on-demand, scalable, device-independent and reliable. Therefore Mobile Cloud Computing, which aims at using cloud computing techniques for storage and processing of data on mobile devices, thereby reducing their limitations. Authentication is the process of recognizing a user's identity[2]. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server.

II. CLOUD COMPUTING

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine. With this technology, the essential sources of a business is often out sourced to a third party, which causes a threat to the security and privacy of data[1].

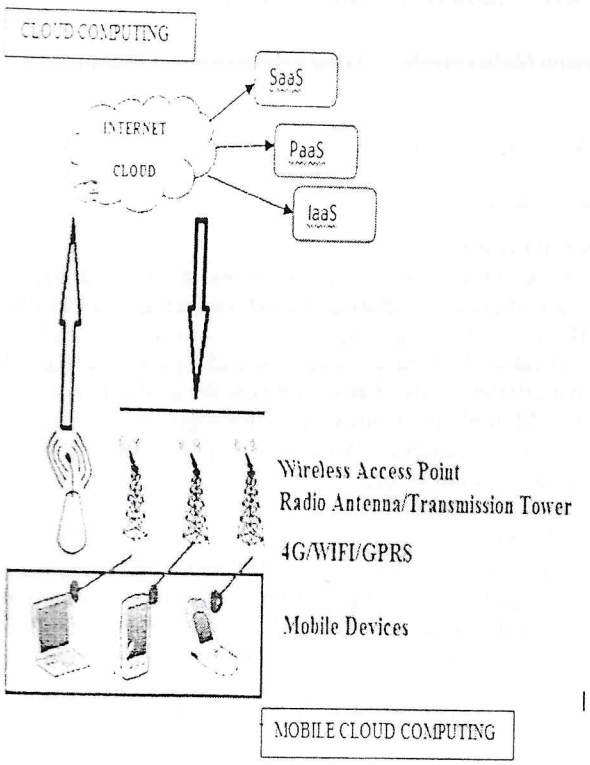
III. MOBILE CLOUD COMPUTING:

Mobile cloud computing means the availability of cloud computing services in a mobile environment . It is a combination between mobile network and cloud computing, thereby providing optimal services for mobile users. Protecting user privacy and data or application secrecy from adversary is a key to establish and maintain consumers' trust in the mobile platform, especially in Mobile cloud computing.

A. ARCHITECTURE

The general architecture of mobile cloud computing can be shown in Figure 1. Mobile networks connect mobile devices via satellite. which control and establish the air links connections and the functional interfaces between the mobile devices and the networks. Mobile users information requests (for e.g., ID, username and location) are transmitted to the central processors which are inter-connected to the servers providing mobile network services. Mobile network operators can provide security services such as AAA (Authentication, Authorization, and Accounting) to the

mobile users based on the Home Agent (HA) and subscribes data stored in databases. Then, the subscribes requests are delivered through the internet to a cloud. The cloud controllers process the requests and provide the corresponding cloud services[1].



Figure(1): Architecture of mobile cloud computing

s shown is the Figure 1, mobile cloud computing can be ...oded into cloud computing and mobile computing. Those ...e devices can be laptops, PDA, smart phones, and so ... with connects with a hotspot or base station by ... WIFI or GPRS. As the computing and major data ...ocessing phases have been migrated to cloud, the ...ability requirement of mobile devices is limited, some ...w-cost mobile devices or even non-smart phones can also ...ieve mobile cloud computing by using a cross-platform ...ware. Although the client in mobile cloud computing is ...anged from fixed machines to mobile devices, the main ...ect is still cloud computing. Mobile users send service ...uests to the cloud through a web browser or desktop ...plication, then the management component of cloud ...ocates resources to the request to establish connection, ...e the monitoring and calculating functions of mobile ...d computing will be implemented.

SERVICE MODEL PROVIDED BY MCC:

Mobile cloud Computing allows user to store ... amount of data to the cloud server with ... reliability, availability and without doing ... management of storage hardware. Mobile ... become an essential part of human life. Demands ... and complex activities require a reliable and ... computing device, Mobile device provide best solution ... mobile cloud computing to solve large complex ... Beside the growth of mobile cloud computing it is ... increase the trust of user in the cloud-based ... management, especially among businesses because of ... risk of security and privacy. The threat becomes an obstacle to adapting mobile cloud computing paradigm. Therefore, it is necessary to build strong security system that can reduce the risks of security and privacy in MCC. There are three types of service model provided by mobile cloud computing to mobile device user. It has increased the productivity of a variety of different fields[2].

a. Software as a Service (SaaS) - It included cloud based software and application such as cloud based antivirus and word processing software. The applications are accessible from various client devices through a web browser[4]. The user does not manage or control cloud infrastructure including network, servers, storage. ex, Yahoo mail, Drop box, Google Docs.

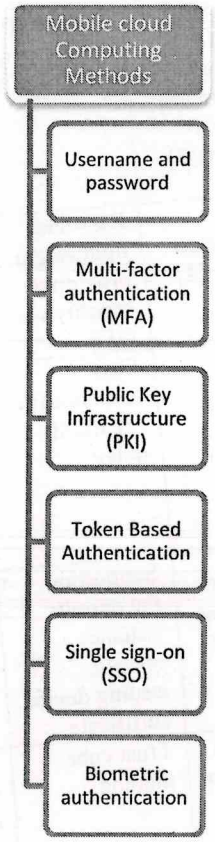
b. Platform as a Service (PaaS) - Platform as a service allows product deployment on the cloud created by consumers using programming techniques and tools[4]. The consumer has control over the deployed applications.eg: Google App Engine, Microsoft Azure, Android (Google Play Store), Facebook.com (application services and online gaming)

c. Infrastructure as a Service (IaaS)
This service provided to consumer to process, store, and perform important basic computing, where client can deploy and run the software freely include operating systems and App. ex. Host firewalls[4].

IV. AUTHENTICATION METHODS IN MOBILE CLOUD COMPUTING:

The data trans- mission between mobile device and cloud server has taken once they authenticate each other, this will ensure secure communication between two legitimate parties. It is not suitable for mobile device to perform authentication process like complex operation because of lack of computational capability.

Different authentication methods in a mobile cloud environment are described in this section. These methods are typically employed to increase security:



Figure(2): Methods of mobile cloud computing

1. Authentication via username and password

The important point in authentication is to protect data from the access of unauthorized people. This entails that the servers reject visit requests from unknown people and manage the access of the confirmed users. In this authentication method, the user should enter the username and password to log in to the system and can then access the information in the cloud.

2. Multi-factor authentication (MFA) :

The traditional authentication method via password cannot sufficiently provide information security against the majority of modern attacks in a cloud computing environment. A secure method is multi-factor authentication. Not only does this method confirm any pair of username/password, but also it requires a secondary factor such as biometric authentication. Of course, the feasibility of the second factor is limited owing to deployment complexity and high expenditure.

3. Public Key Infrastructure (PKI)

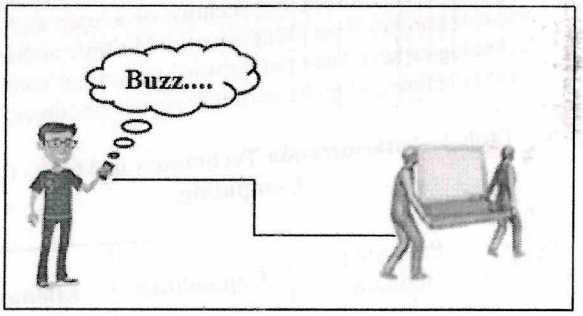
Old authentication systems are based on a hidden key mainly supporting traditional asymmetrical encryption algorithms, such as RSA. It uses a private key to confirm user identity. PKI has been adopted in the design of security protocols such as SSL/TSL and the use of SET mainly to provide authentication. PKI success depends on the control of access to private keys similar to other types of encryption systems. PKI mechanism should provide data confidentiality, data comprehensiveness, non-repudiation, strong authentication, and permit insurance.

4. Single sign-on (SSO)

SSO is an identity management system where a user may be validated in a single authentication and can then access other limited resources without a repeated authentication. In other words, authentication information is generated by using different programs in this method. SSO is a way to access an independent multiple software system where a user logs in to a system and accesses all systems without a need to log in again to a program.

5. Token Based Authentication:

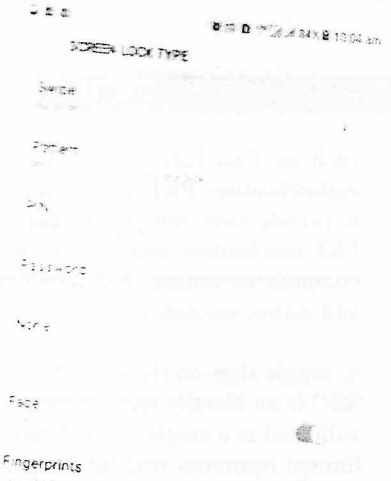
Different authentication tokens have been presented and proposed using cloud computing to secure the data access suitable for mobile environments. Some uses the open standards and even supports the integration of various authentication methods. For example, the use of access or log-in IDs, passwords or PINS, authentication requests, etc.



6. Biometric authentication

Biometric authentication supports three factors of information security, namely authentication, identification, and non-repudiation. This mechanism is based upon the identification of physiological or behavioural characteristics of a person.

A. Physical biometrics: Physical biometrics is a type of authentication based on physical characteristics of human. A major defect of physical biometrics pertains to circumstances where a great number of customers need to be authenticated at the same time. This reduces the speed of the mechanism. There are several physical biometric authentication techniques such as hand geometry recognition, fingerprint recognition, palm print recognition, voice recognition, face recognition, retinal scan, and iris scan. Some of these techniques are of course used in Mobile Cloud computing. some mobile screen shots images are here,



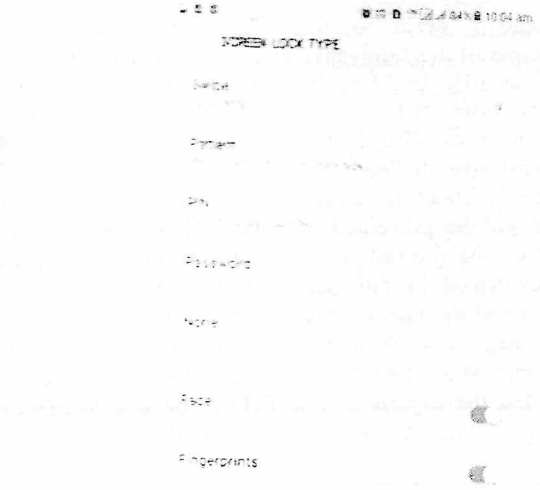
B. Behavioural biometrics: This is based on user behavioural. This technique identifies the users according to their location, typing pattern, profile, etc. Two important types of behavioral biometrics are keystroke analysis, and signature recognition

V. RELATED WORK

Authentication is an important topic in cloud computing security. That is why various authentication techniques in cloud environment are presented in this paper. This process serves as a protection against different sorts of attacks where the goal is to confirm the identity of a user and the user requests services from cloud servers. Multiple authentication technologies have been put forward so far that confirm user identity before giving the permit to access resources.

Table 1: Authentication Techniques in Mobile Cloud Computing

SR. NO.	Presented Solution	Capabilities	Limitations
1	Multi-token Authorization strategy for secure mobile cloud computing [1]	The probability of a token being hacked decreases. As a result, it increases security for the protected resources over the cloud.	The connection link carries the completely distributed token that will be hacked and the hacker can access the protected resources.
2	General authentication plan of a visual password [1]	There is no need to remember a password	Variety in the features of people's natural inform
3	Securing mobile cloud, authentication mechanism via people's fingerprints[3]	Improved performance and security	No log-i allowed t from a use the system.
4	Authentication mechanism [4]	Easy and lightweight, providing security via OTP	Lack of security and time delay
5	Lightweight authentication protocol [5]	Easy authentication , reduced delay	Spending longer time especially for wireless communication s
6	Authentication via mobile phone in a compound cloud [6]	Supporting the permit issuance service, issuing device certificate	RADIUS is unable to provide security services.
7	Framework and its Application to mobile users[7]	Trust cube method	It does not support all devices.
8	Mobile signature for authentication and securing communication [8]	Lightweight mechanism	It cannot identify attacks.
9	Multi-factor authentication using smart phones as the token software[9]	Without external devices Guarantee of OTP generation for each person	User anonymity and accessibility have not been addressed.
10	Biometric authentication[10]	By means of unique pattern (Finger print , Iris , Facial , Retina) create powerful security,	Hard to implement in large scale, need extra cost.



B. **Behavioural biometrics:** This is based on user behavioural. This technique identifies the users according to their location, typing pattern, profile, etc. Two important types of behavioral biometrics are keystroke analysis, and signature recognition

V. RELATED WORK

Authentication is an important topic in cloud computing security. That is why various authentication techniques in cloud environment are presented in this paper. This process serves as a protection against different sorts of attacks where the goal is to confirm the identity of a user and the user requests services from cloud servers. Multiple authentication technologies have been put forward so far that confirm user identity before giving the permit to access resources.

Table 1: Authentication Techniques in Mobile Cloud Computing

SR. NO.	Presented Solution	Capabilities	Limitations
1	Multi-token Authorization strategy for secure mobile cloud computing [1]	The probability of a token being hacked decreases. As a result, it increases security for the protected resources over the cloud.	The connection link carries the completely distributed token that will be hacked and the hacker can access the protected resources.
2	General authentication plan of a visual password [1]	There is no need to remember a password	Variety in the features of people's natural voice information
3	Securing mobile cloud, authentication mechanism via people's fingerprints[3]	Improved performance and security	No log-in is allowed to [illegible] from a user in the system.
4	Authentication mechanism [4]	Easy and lightweight, providing security via OTP	Lack of security and time delay
5	Lightweight authentication protocol [5]	Easy authentication , reduced delay	Spending longer time especially for wireless communications
6	Authentication via mobile phone in a compound cloud [6]	Supporting the permit issuance service, issuing device certificate	RADIUS is unable to provide security services.
7	Framework and its Application to mobile users[7]	Trust cube method	It does not support all devices.
8	Mobile signature for authentication and securing communication [8]	Lightweight mechanism	It cannot identify attacks.
9	Multi-factor authentication using smart phones as the token software[9]	Without external devices Guarantee of OTP generation for each person	User anonymity and accessibility have not been addressed.
10	Biometric authentication[10]	By means of unique pattern (Finger print , Iris , Facial , Retina) create powerful security,	Hard to implement in large scale, need extra cost.

VI. SOME ISSUES IN MCC

Though there are several advantages in mobile cloud ecosystem, there are some issues and challenges in mobile cloud computing. Some of the major issues in security are Data Ownership, Privacy, Data Security and other Security issues [7].

A. Data Ownership

Cloud computing provides the facility to store the personal data and purchased digital media such as e-books, video and audio files remotely. For a user, there is a chance of risk to lose the access to the purchased media data. To avoid these types of risks, the user should be aware of the different rights regarding the purchased media. MCC utilizes the context information such as locations and capabilities of devices and user profiles, which can be used by the mobile cloud server to locally optimize the access management.

B. Privacy

Privacy is one of the biggest challenges in the mobile cloud computing environment. Some applications which hire cloud computing store user's data remotely. Third party companies may sell this important information to some government agencies without the permission of the user. For example: Mobile devices use location based services which help their friends and other persons to get the updates about the location of the user [6].

C. Data Security and other Security Issues

Mobile devices are famous for malicious code. There are many chances to lose or steal the data because mobile devices are mostly unprotected[5]. An unauthorized person can easily access the information stored on the mobile devices. The top mobile threats that affect security are

- Data loss from lost/ stolen devices.
- Information stealing by mobile malware.
- Data leakage through poorly written third party applications.
- Vulnerabilities within devices, OS, design and third-party applications.
- Insecure network access and unreliable access points.
- Insecure or rogue marketplaces.
- Insufficient management tools, capabilities and access to APIs.

VII.CONCLUSION

Mobile Cloud Computing is a combination of wireless network, mobile device and cloud computing. In the field of Information technology, ecommerce, healthcare and transportation etc. have significant benefits of mobile cloud computing. Because of popularity of Mobile devices and its low computing ability MCC have emerge area in the field of technology. The large amount of data storing and data computation occur outside the mobile device. The advantages of this innovative computing model, MCC could suffer security problem because mobile devices access services from different geographical location ,from un trusted network. Therefore, security solutions in this system are constantly updated. A very important part of data security in cloud is authentication, so that unauthorized people will be prevented to enter and merely authorized people will be allowed to enter. Authentication in cloud was fully explained in this paper together with the existing methods and the factors playing a role. The advantages and disadvantages of each method were investigated in order for the people who intend to use the cloud service to become aware and the experts of this field to be able to improve security as much as possible in light of the comparisons made.

REFERENCES

[1] 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.

[2] DeeptiSahu, Shipra Sharma, VandanaDubey, AlpikaTripathi" Cloud Computing in Mobile Applications"InternationalJournal of Scientific and Research Publications, Volume 2,Issue 8, August 2012.

[3] Wikipedia, http://en.wikipedia.org/wiki/MCC_stored data.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] Google books accessed via,http://books.google.com (2016)

[12] R. W. Lucky, "Cloud computing", IEEE Journal of Spectrum, Vol. 46, No. 5, May 2009, pages 27-45.

[13] cloud computing, www.wikipedia.com.

[14]http://www.crn.com/news/cloud/231900862/box-net-one-ups-apple-icloud-with-50-gb-free-cloud-storage.htm

Author Profile

Asst. Professor Mrs. Shinde Manjusha Arun[Bhandare] Department Of Computer Science & I. T. Rajarshi Shahu Mahavidyalaya, Latur (Autonomous) [Maharashtra] E-Mail:smanjusha777@gmail.com Area of Interest: Cloud Computing, MCC, IOT, Network Security.

Asst. Professor Mrs. Jadhav Shrdha Ramesh Department Of Computer Science & I. T. Rajarshi Shahu Mahavidyalaya, Latur (Autonomous) [Maharashtra] E-Mail: jshradha162@gmail.com Area of Interest: Cloud Computing, MCC, IOT, Network Security.