Securing Data with Authentication in Mobile Cloud Environment: Methods, Models and Issues

A.Cecil Donald
Research Scholar in Computer Science,
St. Joseph's College (Autonomous),Tiruchirappalli

L. Arockiam, Ph.D
Associate Professorin Computer Science,
St. Joseph's College (Autonomous),Tiruchirappalli.

ABSTRACT
Mobile Cloud Computing (MCC) is an emerging technology for mobile services gives new horizon to the IT industry and traditional Internet computing paradigm. It integrates the advantages of the cloud computing and the mobile communication environment. It also carries necessary issues related to Network Latency, Limited bandwidth, Availability, Heterogeneity, Privacy and Security, Computing Offloading and Data Access. But security is the main obstacles that obstruct cloud from being widely adopted. These concerns are originated from the public clouds as it holds the sensitive data in which the data owner hesitates to trust. It is so important to segregate assets logically and physically from one another which acts as a key to deploy security policies that address authentication and authorization issues. This paper discusses various security issues related to authentication and Identity Management and the way it works.

Keywords
Mobile Cloud Computing (MCC), Security, Identity Access Control, Authentication

1. INTRODUCTION
Mobile Cloud Computing is a new technology where most of the computation, processing and data storage accompanied with the applications is moved off the mobile device to the centralized, powerful computing platform which is located in the Cloud. The concept of *Mobile Cloud Computing* was introduced after the introduction of the concept of *Cloud Computing* (i.e. mid-2007). It has been pulling the attention of businessmen as a profitable field that reduces the running and development costs of mobile applications and mobile users. This new technology helps to achieve the richer experiences of a variety of mobile services at very low cost and a promising solution for the core IT. Cloud basically provides two main services namely Storage and Computation. Due to the vast increase of Internet access through various devices, it is vitally necessary to have service provider systems, which permits to access various cloud services. Misuse of user's personal information was enforced. These concerns arise from the fact that sensitive data are stored and processed in public clouds, which are operated by third party service providers and shared by various users. There are several advantages in mobile cloud, but at the same time, smart phones approach 100% penetration rate [1]. The very first security threats in the mobile domain came in 2004. Earlier, mobile phones had limited features and relatively protected within the operators. With the emergence of smartphones, the features of mobile phones have taken a new dimension. Now, there are virtually hundreds and thousands of malware and viruses that can potentially affect smartphones. The risk of using common mechanisms has been rising due to the spread of malicious programs like malware, virus and spyware [2]. This presents new security vulnerabilities and complicates matters, given that handsets abide by computational and power limitations and entirely different usability. A recent survey says that large companies had 93% of security threats in the past year, whereas small companies experienced 87% of breaches [3]. This paper discusses the security from the point of view of individual user.

With the above brief introduction, this paper is organized as follows: section 2 discusses the motivation of the paper. Section 3 describes the standard architecture of MCC and workflow of standard authentication. Section 4 describes the barriers of Mobile Cloud Environment. Section 5 presents the various existing architectures and frameworks of MCC. Section 6 brings out the weakness of Security technologies. Finally, section 7 concludes the paper and suggests the future research work.

2. MOTIVATION
Cloud Computing is the combination of web 2.0, Grid Computing, Virtualization, Utility Computing, SOA and Autonomic Computing. Then, what is Mobile Cloud Computing?*Mobile Cloud Computing (MCC) is a new concept that can be simply described as the availability of cloud computing services and resources for mobile devices.* Various authentication mechanisms have been proposed and presented using cloud computing for securing the data access that is suitable for mobile environments.Some providers use the open standards and even support the integration of different authentication methods.For example, the use ofaccess, log-in IDs, PINS or passwords, authentication requests, One Time Password, etc. [4]. Even though MCC possess several advantages, it has some issues since MCC is the combination of mobile networks with cloud computing. A One Time Password (OTP) is an additional layer of security to identify a user which is only valid for a single transaction. On-demandOTP systems such as RFC 4226 [5], involve the use of a server-specific security token that shares a secret key with the server, which not only requires an initialization process such as process, cost and time but also some issues like revealing of token, stolen or lost. This paves the way for the adversary users use it to impersonate the user to the server, at least until it is blocked. The major challenge in the authentication management in networks such as the establishment of Internet based credentials [6]. Building an authentication mechanism using an existing security infrastructure is thus a potentially cost effective approach. The existing security mechanism uses static password authentication infrastructure in which weak passwords are shared by application servers and users. However, this security infrastructure is vulnerable to a number of attacks. As mobile devices establish communication through wireless network, there is no guarantee that the user credentials are securely exchanged. There is the vital need to optimize the authentication process in mobile cloud environment.

3. MOBILE CLOUD ARCHITECTURE

Hong et al. [7] proposed the general architecture of Mobile Cloud Computing shown in Figure 2. Mobile networks connect mobile devices via base stations (i.e. satellite, Access point, Base Transceiver Station (BTS), etc.) which control and establish the air links connections and the functional interfaces between the mobile devices and the networks. Mobile user's 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 subscriber's data stored in databases. Then, the subscriber's requests are delivered through the internet to a cloud. The cloud controllers process the requests and provide the corresponding cloud services. Those services are developed with the concepts of virtualization, utility computing and service oriented architecture (e.g. Database servers and web application).

3.1 Security Technologies in Cloud

User Authentication and Access Control are the two representative security technologies used for cloud platforms. Access Control is a technological process done in OS, not to approach the next process without completion. There are three access control mechanisms in common.

- *Discretionary Access Control (DAC)*
- *Media Access Control (MAC)*
- *Role-Based Access Control (RBAC)*

DAC helps a user to establish the authority to the resources. MAC provides horizontal/vertical access rules at the standards of security. RBAC is the widely used mechanism in commercial organizations, which gives an access authority to a user group based on their role in the organization.

As Mobile Cloud is widely adopted and used by the Business users, it is essential to provide a role based access control mechanisms. Technologies commonly used to authenticate an user are UserId/Password, Public Key Infrastructure (PKI), Multi Factor Authentication (MFA),Single Sign On (SSO), Mobile Trusted Module (MTM) and i-Pin.

3.2 Working of Mobile Authentication:

The standard mobile device authentication is shown in figure 3 which is the basis for mobile cloud authentication.

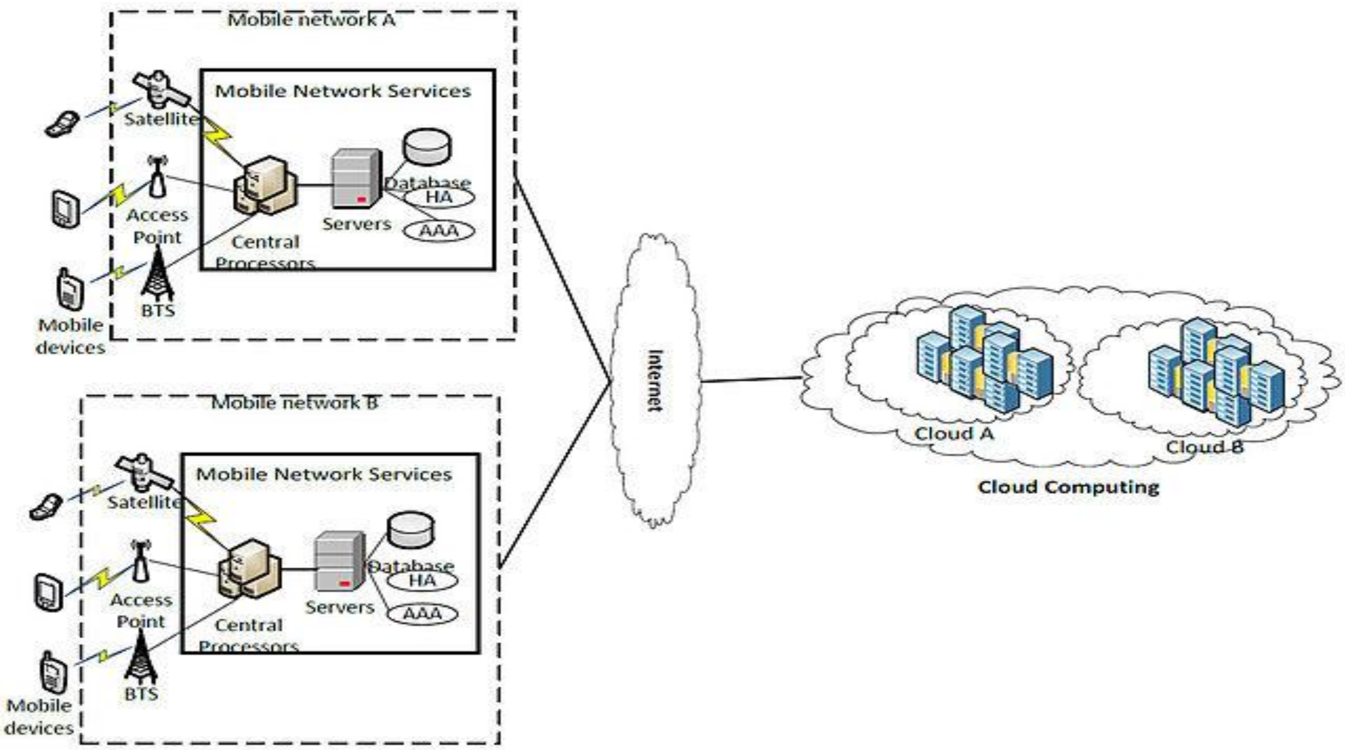

Figure 1.Architecture of Mobile Cloud Computing (MCC) [7]

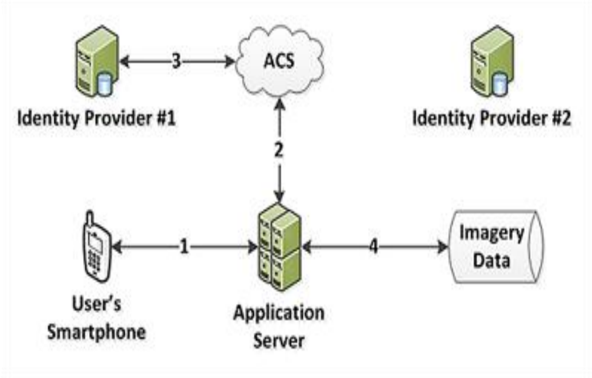

Figure 3: Standard Mobile Authentication [8]

1. At first, Service user launches the mobile application.
2. The client is redirected to a Security Token Service (STS) by the application server in order to perform authentication. (E.g. Windows Azure AppFabric Access Control Service (ACS)).
3. In turn, ACS redirects the service user to the corresponding Identity Provider (IP). Here, Active Directory Federation Services (ADFS) server, which is operated by the user's employer.
4. Once authentication and authorization are successfully completed, the user is allowed to access the requested application data. Then, the data access is audited by the log which is maintained in the application server located in cloud.

4. BARRIERS OF MOBILE CLOUD COMPUTING

There are several issues in Mobile Cloud Environment, when compared to cloud computing. MCC is the combination of mobile communication environment and cloud computing. The security related issues are then divided into two broad categories as listed below.

1. *Mobile Communication Side Issues*
2. *Computing Side Issues*

Issues in Communication Side:

i. Network Latency
ii. Limited bandwidth
iii. Availability
iv. Heterogeneity

Issues in Computing Side:

i. Security and Privacy
ii. Computing Offloading
iii. Context Awareness
iv. Data Accessibility

Several problems that arise need to be taken into account, when making use of cloud computing services on mobile devices. Some of them are,

- Mobility and cloud session connectivity
- Absence of security standards (CIA)
- Unreliability
- Data Storage and Processing Power
- Limited Scalability
- Heterogeneity
- Network Data breaches

5. EXISTING AUTHENTICATION APPROACHES

Several recently proposed Mobile Cloud security frameworks incline to offload the security/privacy related tasks to the cloud. Although this offloads a bulk of the secure data processing overheads to the cloud, mobile devices still need to be involved to perform security operations, such as cryptographic operations and authentication, before outsourcing the sensitive data or tasks. These mentioned security operations still consume considerable amount of energy and might cause performance degradation. This issue can be managed by reducing the amount of data that need to be processed and by optimizing the cryptographic techniques [9].

One of the greatest challenges is device authentication, which means ensuring that only the intended devices are actually communicating. Another way is ruling out the possibility that an unknown device or man-in-the-middle, intercepting the data. This challenge is difficult because devices in ubiquitous computing are not assumed to possess a priori knowledge of each other.

Jones et al. analyzed that, with the help of user name and password, users will sign into the mobile application. To minimize the risk of stolen/shared passwords, it is better to use a multifactor authentication with the combination of user name or password and Radio Frequency Identity (RFID). Even though, the medical field has come in to adopt RFID cards, Smartphones do not possess RFID readers.

Chow et al. [10] proposed a policy based cloud authentication platform. This framework addresses the client device authentication issue in a simple and flexible manner. The proposed platform utilizes the TrustedCube for managing the authentication infrastructure and implicit authentication which helps to translate user behaviors into score. Implicit authentication is referred as behavioral authentication. The behavioral authentication uses habits instead of text data or biometric to authenticate users.Probabilistic authentication scores are assigned to client devices on the basis of observed behaviors with the help of a statistical model. This authentication framework compares threshold values with a user authentication score to identify whether the device is in the hands of a legitimate user or not. But the proposed scheme is dependent on the authentication service to identify a legitimate user. As the user increases, the performance degrades when authentication service is hosted by third party.

Xiao and Gong [11] proposed a lightweight algorithmfor an MCC environment to generate the automatic dynamiccredentials with the mutual coordination of mobile devices andcloud. The automatic generated credentials protect mobile usersfrom an adversary. The proposed scheme changes the dynamic credentialconstantly on the basis of user and cloud communication.The exchanged data between cloud and user are transformed into dynamic secrets.

In a paper, Griffin [12] stated that OTP are one of the methods used in multifactor authentication. Some organizations are worrying a lot about the security in OTP after the high attacks against Data Security (RSA) and some of its users. However, we still consider an OTP as a solution for multifactor authentication, it is widely preferable to the static passwords.

Soo Park et al. [13] proposed a protocol named SSP-M Cloud protocol which comprised of two phases named Smartphone Verification (Mobile) and Cloud Computing Verification (Cloud). Device Verification Server is to control the use of Cloud Computing services in mobile devices and Cloud Verification Server to verify the defect of the Cloud Computing system and application.

Chen et al. [14] proposed an OTP service using Generic Authentication Architecture (GAA) which comprises of UMTS-GAA and TC-GAA. This framework focuses on standard GAA build on the mobile which is supported by the UMTS infrastructure. It is a standardized extension to the mobile authentication infrastructure that enables the provision of security services such as key establishment to network applications.

Anand Surendra Shimpi [15] proposed a secure framework for processing data in mobile cloud computing. This framework stores data in a secured fashion which helps in protecting the user's privacy. In addition, he has implemented a project named "Focus Drive" which improves the driving safety of teenagers.

Yu et al. [16] exploit a novel cryptographic approach using Key Policy-Attribute Based Encryption (KP-ABE) scheme to achieve the secure data access control and data outsourcing storage in the semi untrusted cloud servers. Yu et al. also applied re-encryption scheme in revocation phase to reduce the data cost. In a dynamic mobile cloud, the ABE based approach may not be efficient to provide user access control due to frequent node revocations. The drawback of exploring the ABE as method is the attributes of the data sharers that should be known before encryption.

Weiwei et al. [16] proposed a novel Secure Data Service Mechanism (SDSM), to efficiently achieve both of the access control and data secrecy. Especially, the mobile users can securely shift their data distribution and computing overhead to the cloud. Only authorized users are able to decrypt the cipher text where unauthorized users are not able to read the data.Weiwei et al have also given the security and performance analysis on SDSM which results in the reduced overhead of communication. This reduced the cost of the user side and enhanced the security. But the size of re-encryption key is larger than the data shared by the users.

Richard et al. [17] 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.

6. USER AUTHENTICATION TECHNIQUES AND THEIR WEAKNESSES

This section looks briefly about the security technologies and their weaknesses. Various security issues in mobile cloud environment and the common solutions to those issues are shown in table 1.

Table1. Security Issues and Corresponding approaches in Mobile Cloud Computing (MCC) Environment

Security Issues		Current Approaches
Mobile Terminal	Malware software	Detection and prevention Cloud Antivirus
	Software vulnerabilities (application software; operating system)	Installing the system patches Checking the software legitimacy and integrity
	Others (Lack of security awareness, mis-operation)	Regulating the User's behavior
Mobile network	Information Leakage or Malicious Attack	Data Encryption; Security Protocol
Mobile Cloud	Platform Reliability	Integrating the current security technologies; Key management and data encryption; Authentication and access control privacy and data protection
	Data and Privacy protection	

UserId/Password is the simple, easy and commonly used authentication technique. UserId/Password must be renewed often to make the hacking process more complicated task to the adversarial users.

Public key Infrastructure(PKI) enables a user to authenticate the other party based on the certificate without sharing the secret information. But the major problem is impossible to manage the client side process.

Multifactor authentication is the process of combining two authentication medium such as Id/Password, biometrics (Fingerprint, Iris, Voice, Signature), One Time Pad (OTP), etc. But the problem with id/password and OTP is they can be disclosed to any attacker.

Single Sign On (SSO) is a kind of passport that is provided during the first time authentication. No further authentication is required for an user for other sites/process. SAML is the standard assertion used in SSO.

Mobile Trusted Module (MTM) is the hardware-based security module. It is proposed by the Trusted Computing Group (TCG) in which mobile companies took part in it. It is applied mainly to the authenticate terminal (Mobile Users) from Telecommunications due to the generalization of smartphones.

iPin is also an user authentication techniques used to confirm an user identification. This technique is currently used in korea.

Among all these security technologies, OTP and UserId/Passwords may have key logging attack/SSL strip attack, etc.

7. CONCLUSION

Mobile cloud computing is one of the most emerging mobile technology trends since it integrates the advantages of both mobile communication and cloud computing. It provides optimum services for mobile users. This paper has discussed the standard authentication method, various Authentication issues and models concerning to Mobile Cloud. Securing mobile cloud computing user's sensitive data and accessibility is one of the key issues in which most cloud providers are taking care off. In this paper, various existing authentication techniques have been discussed. Some uses the open standards and even provisions the integration of various authentication methods. From theliterature study, it is essential to develop a lightweight authentication scheme for the mobile cloud environment in which both the security and performance should be maintained / improved. In order to enhance the security of Mobile Cloud Computing, continual research is needed to understand the various types of mobile device communication and cloud computing security threats. Moreover, continued research on new threats and creating a response plan to such threats is necessary to create a safer and more secure user environment for Mobile Cloud Computing.

8. REFERENCES

[1] L. Cheung and C. Newport, "Provably secure ciphertext policy abe", In Proceedings of the 14th ACM conference on Computer and communications security, ACM, 2007, pp 456–465.

[2] D. H. Bae, "A Study on the Revision of the 'Personal Information Protection Act' and its Related Acts", Research of IT and Law, vol. 6, (2012) February, pp. 1-261

[3] http://www.logicworks.net/blog/2013/09/whos-cloud-13-2013/?utm_source=IL&utm_medium=Social&utm_campaign=WhosWho9.13.2013#%21

[4] http://gcn.com/Articles/2013/Cloud_BYOD_enterprise_authentication.aspx?Page=3#

[5] M'Raihi D, Bellare M, Hoornaert F, Naccache D, Ranen O (2005) HOTP: an HMAC-based one-time password algorithm. Internet Engineering Task Force, RFC 4226, 2005.

[6] Soeung-Kon Victor Ko, Jung- Hoon Le and Sung Woo Kim, "Mobile Cloud Computing Security Considerations", April 30, 2012.

[7] Hong T. Dinh, DusitNiyato, Ping Wang and Chonho Lee," A Survey of Mobile Cloud Computing: Architecture, Applications and Approaches", http://onlinelibrary.wiley.com

[8] http://cloudsecurity.techtarget.com/tip/Password-based-authentication-A-weak-link-in-cloud-authentication

[9] Dan Griffin and Tom Jones, "Designing a Cloud Based Mobile Application for Compliance", In Proc. of security TechCenter, October, 2013.

[10] Reza Rahimi, Jian Ren, Chi Harold Liu, Athanasios V. Vasilakos, NaliniVenkatasubramanian, "Mobile Cloud Computing: A Survey, State of Art and Future Directions", Proceedings of Mobile Network Applicatons, Springer, 2013, DOI 10.1007/s11036-013-0477-4.

[11] 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.

[12] Donald, A. Cecil, S. Arul Oli, and L. Arockiam. "Mobile Cloud Security Issues and Challenges: A Perspective." International Journal of Electronics and Information Technology (IJEIT), ISSN (2013): 2277-3754.

[13] 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, DOI: 10.1007/978-94-007-2598-0_18, pp. 165-172.

[14] 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, 2013, pp. 738-747.

[15] http://www.h-online.com/security/news/item/Three critical-vulnerabilities-in-Kerberos-network-authentication-732601.html.

[16] C. Wang, S. Yu, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing", In Proc. of INFOCOM, IEEE, 2011, pp.534–54.

[17] 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.