A Unified Cloud Authenticator for Mobile Cloud Computing Environment

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

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

ABSTRACT

Mobile cloud computing (MCC) is just cloud computing in which at least some of the devices like mobiles, PDA etc are involved. This paper drives over several authentication techniques and methods for mobile cloud computing. An analysis of the existing works are carried out. This Paper also analyses the attacks and Issues that occur during authentication in the mobile cloud environment. Security is the main issue that obstructs cloud from being widely adopted. A framework called the Mobile Cloud Authenticator (MCA) is proposed for authenticating the mobile users in the mobile cloud environment. The overall framework of MCA consists of three major entities namely, Cloud users, Mobile network and Cloud. There is a system called Unified Cloud Authenticator (UCA) which is placed in between the mobile network and Cloud Service Provider (CSP). It authenticates both users and CSP. The UCA contains Authentication Server (AS), hashing machine, connection manager, user manager and service manager. The operational procedure of UCA has three phases namely registration phase, authentication phase and verification phase. This paper explains the overall framework of MCA and the functions of UCA in detail.

Keywords

Mobile Cloud, Mobile Cloud Authenticator (MCA), Unified Cloud Authenticator (UCA), Authentication

1. INTRODUCTION

In recent years, there is a noteworthy increase of mobile subscriptions due to the quick advance in wireless, mobile and networking technology. Mobile Cloud Computing has been dragging the attention of businessmen as a profitable field that reduces the running and development costs of mobile applications and mobile devices. The concept of Mobile Cloud Computing was introduced after the introduction of the concept of Cloud Computing (i.e. mid-2007).

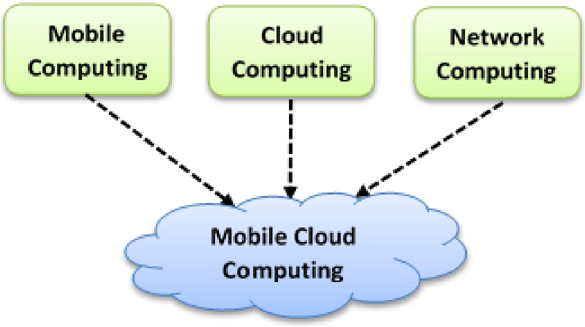

Figure 1. Evolution of Mobile Cloud Computing

Mobile Cloud Computing integrates the major concepts namely: Mobile Computing, Cloud Computing and Network Computing as shown in figure 1. The primary objective of the MCC model is to take the advantages of cloud computing and apply it to the mobile environment. It utilizes the cloud only when it is advantageous i.e. improves performance or reduces resource utilization, or provides robustness, leverage scalability and location-awareness of cloud platforms. According to TechNavio analyst's prediction, the Enterprise Mobile Cloud market will grow 18.12% in 2011–2015 [1]. One of the key factors paying for this growth is the demand for enterprise mobility. The primary vendors controlling this market space include IBM, Amazon, Terremark Worldwide and Salesforce.com. Mobile devices are important for ubiquitous access to data, especially remote data accessibility because the modern smartphone and tablet devices support heterogeneous network interfaces such as Wi-Fi, Bluetooth, 3.5 or 4G and so on [2]. While the mobile terrain has captured the front-end deployment of the most modern architectures, the cloud computing platforms have also established dominance as the back-end layers. Thus, mobile cloud computing has become the focus of most studies recently. There are numerous advantages in mobile cloud, but at the same time, mobile approaches 100% penetration rate. The very first security threats in the mobile domain came in 2004. Now, there are almost hundreds and thousands of malware and viruses that can possibly affect smartphones.

According to the IDC survey, 74% Chief Information Officers and IT managers consider that security and privacy issues are the main hurdle in preventing organizations to adopt cloud computing services [3]. In March 2009, a bug caused Google caused documents to be shared without the owner's knowledge [4]. The main reason is Cloud Service Providers (CSP) typically work with many third party vendors and there is no guarantee as to how these vendors safeguard data. It is to be noted that this security breach have occurred in the top horsemen's organization and it is essential to protect the user data in mobile cloud environment.

With the above brief introduction, this paper is organized as follows: section 2 discusses review of the Literature. Section 3 lists out the attacks that happen in MCC. Section 4 enlists the issues and challenges in MCC. Section 5 presents the motivation of the paper work and Section 6 presents the proposed Mobile Cloud Authenticator (MCA) framework and its working procedures in MCC. Finally, section 7 concludes the paper and suggests the future research work.

2. REVIEW OF LITERATURE

Several user authentication mechanisms are provided by researchers to improve security in mobile cloud environment.

Omri et al. [5] presented an application that uses handwriting recognition as an authentication pattern to certify access in mobile cloud. In this mode, the user is recognized by password and unique handwriting style. The diligence, which utilized the smartphone as a biometric capture device and also used Hadoop to set up the link between mobile users and the cloud via the Internet. It has been carried out in two ways. The primary difference is in the execution manner, i.e. one as a web page and the other as a mobile application.

Rassan et al. [6] projected a solution for authenticating mobile cloud consumers using the prevailing mobile device camera as a fingerprint feeler to get a fingerprint image, process it and realize it. Their results indicate that the proposed solution has additional importance to sustain functioning at an assumed degree. The author indicates the future work for accessing log file can be used to identify unauthorized attempts to access data by third party cloud providers or any hackers. Based on the activity logs, cloud security policies shall be revised and re-configured.

Xiao and Gong [7] proposed an authentication algorithm for the Mobile Cloud environment to produce the automatic dynamic credentials with the mutual coordination of mobile devices and cloud. The automatically generated credentials protect mobile users from an adversary. The proposed scheme alters the dynamic credential persistently on the basis of cloud communication and the user. The exchanged data between user and the cloud are converted into dynamic secrets. The chance of attack seems to be impracticable due to mobility, user, resource limitation and unreliability of wireless communication. Even the loss of a single packet makes the recovery so critical.

In the paper [8], Yan Zhu have proposed a cryptographic access control framework for Location Based Services (LBS) on mobile cloud. This framework facilitates fine-grained access control, location based authentication, and privacy protection. It is based on a spatial-temporal predicate-based encryption (ST-PBE) scheme which implemented a secure cryptographic integer comparison mechanism to support various predicates required in LBS. In addition, the implementation of a proof-of-concept prototype and corresponding evaluation demonstrate the feasibility of their methodology.

Kai et al. [9] proposed an efficient bio-cryptographic security protocol intended for client/server authentication in the present mobile computing environment, with a realistic assumption that the server is secure. In this protocol, fingerprint biometric is used in user verification, protected by a computationally efficient Public Key Infrastructure scheme, Elliptic Curve Cryptography. The candid information of the fingerprint is hidden in the feature vault, which is the mixture of candid and chaff features. The features of the Fingerprint are not only used for biometric verification but also for a cryptographic key generation. The analysis of security shows that the projected protocol can afford a secure and trustworthy authentication of isolated mobile users over insecure network. Investigational results on public domain database show an adequate verification performance. They have also tested and evaluated the computational costs and efficiency of their protocol on the CLDC emulator with Java programming technology. The simulation outcome proved that the proposed protocol outfits the current mobile environment.

Thamba et al. [10] said that the biggest challenge in both cloud and mobile technologies right now is security. MCC combines the two technologies and have a security wormhole. They presented the current state of mobile-cloud authentication technology and their proposed system Mobile Cloud Key Exchange (MCKE), an authenticated key interchange pattern that aims at efficient authentication. This pattern is aimed on randomness reuse scheme and Internet Key Exchange (IKE) pattern. Theoretical analysis and simulation results are compared with the IKE scheme. The MCKE system can considerably improves the efficiency by intensely reducing the time consumption and the computation load without losing the level of security. This scheme is not efficient for larger databases, as it consumes a lot of time and computation load. Therefore, as future work investigations can be done on new strategies to improve the efficiency of symmetric-key encryption headed for more efficient security-aware scheduling.

Majid et al. [11] introduced a method of authentication which is capable of identifying users based on Keystroke Dynamic Authentication. Moreover, keystrokes duration is calculated as an aspect for measuring keystrokes of mobile's consumers. A strong password authentication scheme is proposed by integrating the keystroke authentication with password, which is a kind of behavioral biometric mechanism. Investigational results show that, the projected scheme can work 97.014% appropriately because the keystroke duration of each user hang on their behavior characteristic and it can be dignified up to milliseconds (ms). On the other hand, if an unauthorized person knows the user name and password of legal user, one cannot gain access rights because of the difference between their keystroke duration.

Revar et al. [12] describe the usefulness of single sign-on in a mobile cloud computing environment [6]. Single sign-on (SSO) is used on the top layer of cloud. They verified the single sign-on authentication scheme on an Ubuntu server. In SSO, a single user name and password combination is used to access multiple cloud applications. This scheme does not address exactly how a mobile device or any cloud compatible device will access the cloud using SSO.

Khan et al. [13] introduced a light-weight dynamic credential generation scheme for mobile-cloud-computing environment. The dynamic credentials are generated on the basis of cloud-mobile communication that can provide better protection against credential faking or stealing attacks. The experimental results show that the proposed scheme significantly improves the turnaround and energy consumption of the mobile device as compared to existing schemes. Furthermore, the proposed scheme works accurately even in the presence of a fully distrusted cloud environment. In addition, the proposed scheme reduces the possibility of the Man-in-the-Middle attack due to the involvement of nonce in generating the cloud and mobile secrets. To ensure the legitimacy of the mobile user in the proposed scheme, the manager authenticates the mobile users before forwarding the dynamic credentials. The mobile users can also verify the credibility of the credential with the help of received signature. Also, the credentials are encrypted with the mobile user public key that ensures the confidentiality.

In the multilevel authentication system proposed in [14], authentication method creates and authenticates the password at multiple levels to provide access to the cloud services. Access is allowed only if the authentication is successful at all levels.

- The first level of authentication is the organizational level. This level reads out the organization password; if unauthenticated, the process will terminate. If it is authenticated, then it enters into second-level authentication.
- Second level of authentication is the team level. This level reads out the team password; once authentication is done, it then enters into user level authentication.

- Last level is the user level. In order to provide the user privileges and permission, this level reads out the user's password.

This section reveals the literature study related to the authentication in MCC, which clearly shows how the proposed mechanisms failed to protect the user credentials.

3. SECURITY THREATS IN MOBILE CLOUD ENVIRONMENT

It is necessary to understand security threats in Mobile Cloud Environments to propose an authentication system suitable for Mobile Cloud services. So, the threats are divided into four kinds as follows.

3.1 Man-in-the-Middle attack

This threat happens between the authentication server on the internal network and outside user such as smartphone, tablet, etc. Generally, a user connects the RADIUS server for checking the user identification information and RADIUS server checks the user and user's device identification. When an attacker uses cheat user information in the intranetwork or the attacker can try by masquerading his individual information against user's identification information (man-in-the middle-browser attack).

3.2 DoS or DDoS attack

DoS (Denial of Service) is also known as DDoS (Distributed Denial of Service) attack which can happen at the internal network by inside user. Furthermore, mobile environment has several vulnerabilities as the software security check, memory management and deployment of the applications are not completed. So, an attacker can add DoS or DDoS agent into the mobile device easily. During the time of the attack, many mobile devices on the outside network will attack the cloud service server. This is also known as Zero-day attack skill.

3.3 Location Certification attack

Mobile devices move frequently outside the network. But, mobile device location information is very important for its certification. RADIUS server cannot solve every authentication problem for mobile devices. Amongst many authentication dangers, location based authentication glitches are very important in the mobile communication environment because the location information is one of the component of token.

3.4 Script attack

This attack is created by the inside attacker. Every internal user is not a trusted user. Somebody can violate authentication server, VPN server or cloud service server by stealing and altering the user's information. So, this is one of the major problem in cloud service when accessed through mobile devices such as smart phones and tablets.

As discussed above, the vulnerabilities can occur in the cloud computing environment with mobile devices.

4. ISSUES AND CHALLENGES IN MOBILE CLOUD COMPUTING

From the comprehensive literature review of existing and proposed frameworks of MCC explained in section 2, it is evident that there are some major issues and challenges of MCC. Those issues and challenges are highlighted and categorized below. The security related issues are then divided into two broad categories as listed below.

- Mobile Cloud Infrastructure Issues
- Mobile Cloud Communication Channel Issues

4.1 Mobile Cloud Infrastructure Issues

From 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
- Hybrid Cloud Security Management Issues

4.2 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. MOTIVATION

As seen in the above sections, there are only a few proposed systems in the mobile cloud, but for regular cloud there are several proposed schemes that are upright for refining security in regular cloud environment, but in the mobile cloud it's so hard for users because of its limitations and resource constraints. There are several attacks and issues that occur while accessing the cloud using mobile devices. To attract potential customers, the cloud providers have to target all the security issues to provide a completely secure environment. MCC is based on Mobile Computing and Cloud Computing, all the security threats are inherited in MCC with an additional limitation of resource constrained mobile devices. Already existing threats are taken into account in all cloud security architectures. It is still an open problem about how to construct a secure architecture for the mobile cloud environment. The stability between usability and security must be identified, just as when trying to apply the authentication scheme from an outdated client/server to cloud computing. It has a high risk when applied to the outdated client/server because the cloud infrastructure is shared among users and managed by the cloud service providers. It is essential to ensure the authentication as it is the doorstep for the users in a cloud environment. In a mobile cloud computing environment, if a mobile device is registered with a particular cloud service provider, both mobile device and cloud server must authenticate each other in a uniform way. This is to secure the communication with a single authentication technique each time when the mobile device accesses the cloud from different locations using different networks and different mobile devices. A single and secure authentication process will help in preventing third parties from posing as a legitimate mobile device or as a legitimate cloud service provider.

6. PROPOSED FRAMEWORK

Figure 2 illustrates the proposed Mobile Cloud Authenticator (MCA) framework for authenticating the users in the Mobile Cloud Environment. The proposed Mobile Cloud framework comprises of four major components: Users, Mobile Networks, Unified Cloud Authenticator (UCA) and Cloud Service Provider (CSPs). The primary mode of communication from the mobile is HTTP over Wi-Fi while the communication between the Unified Cloud Authenticator and the Cloud Service Provider (CSPs) is over HTTPS. The working procedure of the proposed framework is given as follows. Initially, the user's requests are communicated over the Mobile Networks (MN) which holds the Base Station (BS), AAA sever and a user repository. Base Station acts as the transmitter and the AAA server authenticates those requests in the MN.

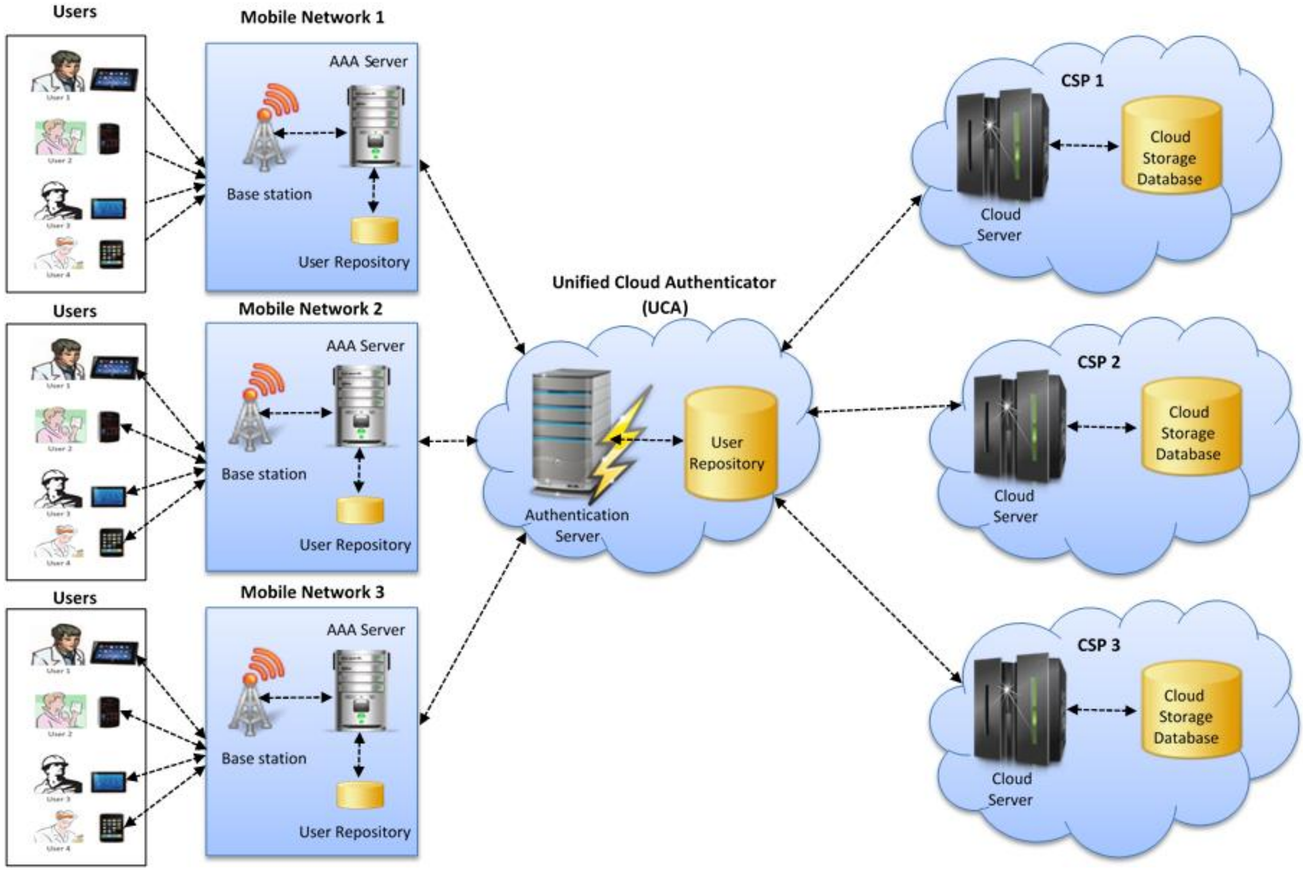

Figure 2. Mobile Cloud Authenticator (MCA)

Then, the requests are directed to the Unified Cloud Authenticator (UCA). The CUS plays the major role in security which contains the Authentication Server (AS) for authenticating not only users but also their roles for accessing their respective services. The user repository is the place where all the user credential data are stored. Another major component is Cloud Service Provider (CSP) who provides the service to the users, which obviously holds the Cloud Service Server and the Cloud Storage Repository.

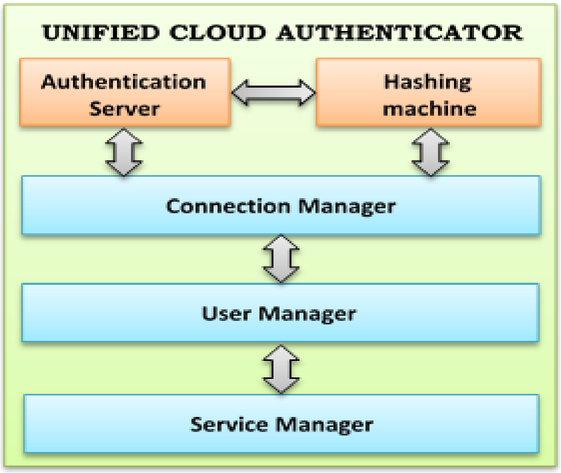

Figure 3. Unified Cloud Authenticator (UCA)

6.1 Components of UCA

There are five components in the UCA which are duplicated in figure 3. All the components are elaborated as follows.

6.1.1 Authentication Server (AS)

Authentication Server plays the vital role in the UCA. All the credentials of the user and the CSPs data are stored in the repository and maintained by the Authentication server. The authentication Server is connected with AAA Server and the CSP for accessing those credentials.

6.1.2 Hashing Machine

Hashing machine is mainly used for hashing the credentials before storing it to the repository. It also generates the random number used for key generation process at the time of the authentication process.

6.1.3 Connection Manager

Connection Manager is used for managing and monitoring the connections during the authentication.

6.1.4 User Manager

User Manager manages the user and monitors them during the authentication.

6.1.5 Service Manager

The service Manager monitors the services accessed by the user.

All the authentication activity logs are maintained in the repository of UCA.

6.2 UCA Operations

The working procedure of Mobile Cloud Authenticator is divided into three phases namely

- *Registration Phase*
- *Authentication Phase*
- *Verification Phase*

The following steps occur during the authentication process.

6.2.1 Registration Phase

This phase is the initial phase that is carried out at the both user and UCA Side.

- Initially, the user registers for accessing the cloud services.
- The username and a password are registered by the user for accessing the services in the cloud.
- Those credentials are maintained in the UCA and a message digest operation will be performed on the user credentials and on the cloud access rights called as MD_{user} and MD_{cloud}. MD_{user} contains the attributes like Username and password and other attributes too. MD_{cloud} contains the Roles for accessing the services and other related information. These operations are performed by the AS and hashing machine.

6.2.2 Authentication Phase

This is the second major phase, which is carried out at the UCA Side.

- A Key K1 is generated using the Username and password given by the user.
- Then, a random number is generated using the Key K1 which is used to generate the Authentication Key A1.
- Authentication key A1 encrypts the MD_{user} and MD_{cloud} called as E1. MD_{user} and MD_{cloud} are generated during the registration phase itself.
- Finally, K1 encrypts the already encrypted E1 (KE1).
- Finally, the KE1 is sent to the user.

6.2.3 Verification Phase

Verification is the process of ensuring the accuracy, correctness or the truth of the information of the user. This phase is carried out at the CSP Side.

- After matching the encrypted key KE1, the CSP sends a Digital Signature (DS) to the mobile user which holds the MD_{user} and MD_{cloud} called as Encrypted Digital Signature (EDS).
- Then it is sent to the user’s mobile in an encrypted format.
- Finally, Mobile device decrypts the EDS with the help of public key PK1.
- The PK1 was generated at the time of generation of KE1.

Thus, the User and the Cloud CSP are verified in the Mobile Cloud Environment.

7. CONCLUSION

In recent times, the Mobile Cloud Computing is becoming a new hot technology and the security has become a research importance. In this paper, several authentication techniques and methods for mobile cloud computing are discussed. This Paper has also analyzed the attacks and Issues that occurred in the mobile cloud environment. A new framework called the Mobile Cloud Authenticator (MCA) is proposed for authenticating the mobile users in the mobile cloud computing environment. The MCA holds the Unified Cloud Authenticator (UCA). The UCA is comprised of Authentication Server (AS), hashing machine, connection manager, user manager and service manager. UCA authenticates both the user and the Cloud Service Provider (CSP). The UCA performs the registration of users, authenticating and verifying them. The proposed MCA framework protects the user credentials and prevents the adversarial users from the unauthorized access of cloud services. This framework ensures the authenticity of the mobile users in the Mobile Cloud Environment.

8. REFERENCES

[1] Ruay-Shiung Chang, Jerry Gao, Volker Gruhn, Jingsha He, George Roussos and Wei-Tek Tsai, “Mobile Cloud Computing Research – Issues, Challenges, and Needs”, Seventh IEEE International Symposium on Service-Oriented System Engineering, IEEE, 2013, ISSN: 978-0-7695, pp. 442- 453.

[2] Richard K. Lomotey and Ralph Deters, “SaaS Authentication Middleware for Mobile Consumers of IaaS Cloud”, Ninth World Congress on Services, IEEE, 2013, ISSN: 978-0-7695, pp. 448-455.

[3] 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.

[4] 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, pp. 1-261.

[5] Abid Shahzad and Mureed Hussain, "Security Issues and Challenges of Mobile Cloud Computing", International Journal of Grid and Distributed Computing (IJGDC), Vol. 6, No. 6, 2013, ISSN: 2005-4262, pp. 37-50.

[6] IehabALRassan and HananAlShaher, "Securing Mobile Cloud Using Finger Print Authentication", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.6, November 2013, pp.41-53.

[7] S. Xiao, W. Gong, "Mobility can help: protect user identity with dynamic credential", In. Proc. of 11th Int. Conf. on Mobile Data Management, MDM '10, 2010.

[8] Yan Zhu, Di Ma, Dijiang Huang and Changjun Hu, "Enabling Secure Location-based Services in Mobile Cloud Computing", In: Proc. International Conference on Mobile Cloud Computing (MCC '13), ACM, August 2013, pp 27-32.

[9] Kai xi, tohari ahmad, fengling han and jiankun hu, "A fingerprint based bio-cryptographic security Protocol designed for client/server authentication in Mobile computing environment", Special issue paper Security and communication networks, Wiley Online Library, 2010.

[10] Thamba Meshach and K.S. Suresh Babu, "Secured and Efficient Authentication Scheme for Mobile Cloud", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 2, Issue 1, February 2013, ISSN: 2319 – 1058, pp. 242-248.

[11] Majid Bakhtiari, Mahnoush Babaeizadeh and Mohd Aizaini Maarof, "Keystroke Dynamic Authentication in Mobile Cloud Computing", International Journal of Computer Applications (IJCA), Volume 90, No. 1, 2014, ISSN: 0975 – 8887, pp. 29-36.

[12] H. Dinesha and V. Agrawal, "Multi-level authentication technique for accessing cloud services," In Proc. of International Conference on Computing, Communication and Applications (ICCCA' 12), 2012, pp. 1-4.

[13] Abdul Nasir Khan, M.L. Mat Kiah, Sajjad A. Madani, Atta ur Rehman Khan, Mazhar Ali, "Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing", Journal of Super Computers, Springer, Vol. 66, June 2013, ISSN: 1687–1706, pp. 1687-1706.

[14] Reza Rahimi, Jian Ren, Chi Harold Liu, Athanasios V. Vasilakos and Nalini Venkatasubramanian, "Mobile Cloud Computing: A Survey, State of Art and Future Directions", In. Proceedings of Mobile Network Applicatons, Springer, 2013.

9. AUTHOR'S PROFILE

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 at St. Joseph's College (Autonomous), Tiruchirappalli affiliated to Bharathidasan University, India. His main area of research is Mobile Cloud Computing. He has published four papers in the International Journals with impact factor and also he has atteneded several national and international conferences and workshops.

Dr. L. Arockiam is working as Associate Professor in the Department of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 25 years of experience in teaching and 18 years of experience in research. He has published more than 187 research articles in the International & National Conferences and Journals. He has also presented 2 research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has authored 3 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 and ASDF Global "Best Academic Researcher" Award from ASDF, Pondicherry for the academic year 2012-13 and also the "Best Teacher in college" award for the year 2013 & 2014.