MoClo-IdM: A Framework for Secured Data Access in MobiCloud Environment

[1] **A. Cecil Donald,** [2] **Dr. L. Arockiam**

[1] Doctoral Research Scholar in Computer Science, St. Joseph's College (Autonomous),
Tiruchirappalli, Tamil Nadu, Country

[2] Associate Professor in Computer Science, St. Joseph's College (Autonomous),
Tiruchirappalli, Tamil Nadu, Country

Abstract - Cloud Computing (CC) is an emerging technology. Mobility is considered as a key technology in CC that shifts from traditional PC to smartphones, tablets, PDAs, etc. MobiCloud has arose as a subclass of CC to empower rigorous on-demand elastic computing and storage to the mobile users. As MobiCloud integrates CC with mobile computing and networks, all the issues are inherited while accessing the cloud services. Many researchers proposed security mechanisms, but not as a complete framework. The existing mechanisms could not perform well due to issues like security, computation overhead and poor accuracy. To overcome these problems, an IdM framework is designed to authenticate and authorize user's data access in MobiCloud environment. The proposed IdM framework incorporates three mechanisms namely Key Based Mutual Authentication (KBMA), Pattern Based User Authentication (PBUA) and Optimized Role Based User Authorization (ORBUA). The three proposed mechanisms are given as a single service called Identity as a Service (IdaaS) by the CSPs. This MoClo-IdM framework can be used by the small, medium and large scale service providers.

Keywords – *Mobile Cloud Computing, Security, Data Access, Identity Management (IdM), Authentication***.**

1. Introduction

The MCC is a rising, revolutionary paradigm that creates an intelligent atmosphere and improves quality of life by leveraging the event of assorted technologies like Cloud Computing (CC), wireless communications, mobile computing and handheld devices, etc. These technologies have already created and leveraged the potential for a globally interconnected mobile environment to supplement their services across multiple cloud providers. According to TechNavio analyst's prediction [1], the enterprise MobiCloud market will grow 18.12% in 2013–2018. At the same time, over 2,50,000 mobile users were compromised in an unprecedented mobile attack. Although the MCC has an excellent potential to facilitate access of powerful and reliable resources anywhere, there are many problems that ought to be considered, together with security and privacy in MobiCloud environment.

A lot of researchers have proposed numerous access schemes based on traditional password, steganography, biometric, etc. with varied efficiencies. However, several of them are prone to numerous attacks and consumes energy within the resource constraint mobile devices. Identity Management (IdM) is responsible for IdM tasks such as allowing a user to establish links between various identities. As cloud is a federated and distributed environment, it is a tedious task to determine the access rights to the user. There is a need for a good combination of architecture and also the use of better security mechanisms which includes the cryptographic techniques too.

The ultimate aim of this research is to present issues in accessing the MobiCloud services and to develop an architectural IdM framework for secured data access in MobiCloud environment. The primary objective is to provide an Identity Management (IdM) framework that incorporates two major processes namely authentication and authorization. The followings are the approaches to achieve the objective.

- To develop an architectural framework to provide secured data access in MobiCloud environment.

- To give a brief explanation of the methodology used in the proposed architecture.
- To explain the significance of the proposed work.

2. Related Works

Though, the researchers have contributed much to the world of Mobile Cloud, they have still indicated some areas for the improvement of future secure MobiCloud environment. An important challenge identified in MCC environment is the lack of an effective IdM system, which can meet the secure access of data or resources. To overcome this issue, a number of researchers have proposed various mechanisms to authenticate the users and authorize the user's data access in MobiCloud environment.

Alizadah et al. [2] did a survey on various authentication mechanisms in MCC environment. They analyzed that the lack of secure and efficient authentication methods necessitate a vital need to develop a suitable authentication for MCC. They have also stated that the future authentication method should minimize the security threats in MCC. Xio et al. [3] claim that the existing IdMs are insufficient against attacks because the adversarial users could steal/fake the credentials. The authors have also proposed an algorithm that generates the dynamic credentials. Their system is secure against Intrusion Detection System (IDS), network firewalling, etc. However, their algorithm is insecure if the IdM server is compromised.

Angin et al. [4] presented that the OpenId has several security flaws and prone to malicious code attack. A malicious code is injected on the server that uses OpenId. This then acts as the bogus identity provider authentication page which asks for credentials. It is prone to timing attack. Few researchers [5] [6] presented an application-centric approach for user authentication. These approaches permit the IDM server to keep track of users' activities to be able to authenticate users without exposing their real identities. Other researchers [7] [8] modify PC-based IDMs to secure user's data on the cloud, however, these modifications fail to address the mobile security challenges. The OpenId and OAuth [9] are the widely used IdMs in cloud environment. OpenId uses the Single Sign-On (SSO) which facilitates login to multiple sites which is vulnerable to attacks like malicious code injection attack, timing attack, etc.

Many researchers proposed the security mechanisms, not as a complete framework. The existing mechanisms could not perform well due to security issues and higher in computation and poor accuracy. From the comprehensive literature review, it is evident that a complete, secure IdM framework for MobiCloud environment is the need of the hour.

3. Structure of MoClo-IdM Framework

In this framework, MoClo-IdM, three mechanisms are integrated to perform IdM functions in MobiCloud environment to provide data access. The mechanisms are [10] Key Based Mutual Authentication (KBMA) for entity authentication, [11] Pattern Based User Authentication (PBUA) for user authentication and Optimized Role Based User Authorization (ORBUA) for user authorization which are playing vital role in MobiCloud environment. These three proposed mechanisms are integrated and a new complete architectural framework is developed. All these three mechanisms are developed by three different procedures. The aim of the framework is to provide secured access to the data in MobiCloud users.

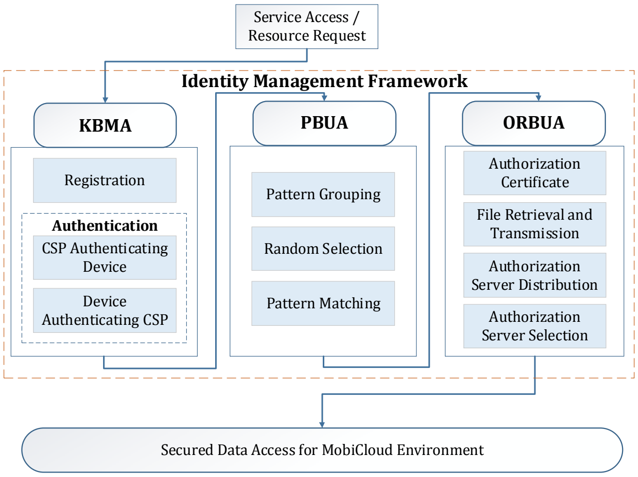
Service Access / Resource Request
Identity Management Framework
KBMA
Registration
Authentication
CSP Authenticating Device
Device Authenticating CSP
PBUA
Pattern Grouping
Random Selection
Pattern Matching
ORBUA
Authorization Certificate
File Retrieval and Transmission
Authorization Server Distribution
Authorization Server Selection
Secured Data Access for MobiCloud Environment

Fig. 1 Structure of MoClo-IdM.

The structure of the framework, MoClo-IdM and their components are depicted in fig 1. Each proposed mechanism has different procedures for specific purposes.

3.1 Key Based Mutual Authentication (KBMA)

KBMA has been proposed to authenticate the entities involved in accessing the resources in MobiCloud environment. All the communication takes place between the entities. As all the communications in MobiCloud environment takes place over the wireless network, there is a possibility for a hacker to masquerade the communication messages. The hacker uses the captured messages to access the MobiCloud resources.

KBMA has been developed by having two different processes namely registration and authentication processes. Registration process is a one-time process for setting up an account for accessing MobiCloud resources. This process is carries out through SSH v2. The authentication process is to authenticate the entities mutually. It is subdivided into two activities namely; CSP authenticating Device and Device authenticating CSP. The algorithm of the KBMA is analyzed using the Scyther tool. The derived results show that the proposed KBMA is resilient against masquerading attack, man-in-the-middle attack and the claims of the security is also analyzed. From the results, it is evident that the proposed authentication mechanism is more secure.

3.2 Pattern Based User Authentication (PBUA)

Most of the cloud players use traditional system such as static passwords, biometric, digital certificates, etc. to authenticate the users. These existing mechanisms are prone to shoulder surfing attack and some mechanisms need high computation which consumes more time. To overcome these issues, PBUA is proposed to authenticate the users in MobiCloud environment. This user authentication process occurs only after completing the KBMA operations (i.e. mutual authentication).

Two processes take place in this mechanism namely user identification and authentication. Initially the user is identified to reduce the time and authentication is done using dynamic pattern sequences. The patterns are matched using the hash-based technique to reduce the complexity and increase the efficiency. Patterns are generated dynamically to prevent shoulder surfing attack. The interpretation results show that the complexity is reduced by $1/n^2$. Thus the efficiency is improved by n^2.

3.3 Optimized Role Based User Authorization (ORBUA)

Cloud enables users to store huge amounts of data and to perform several computations on it. The cloud users not only involve in operating on the data, but also involve in sharing the data and resources with other users. The major advantage of using MobiCloud technology is the availability of large storage space and the possibility of data sharing. In such an environment, protecting the data becomes a major concern. Security can be enhanced by providing access control to the authorized users. Access control provides authorization to the users by providing access levels for users requiring to operate on the data or the resources. ORBUA deals with providing an effective and distributed solution to perform cloud access using mobile devices. Here, the user performs only two transmissions; first is to obtain the authorization certificate from the owner and the second is to provide file or resource request to the Authorization Server. Both the transmissions are encrypted, hence the probability of attacks is lowered. The major advantages of the proposed model is that the computations in the user side is reduced to a large extent and transmission requests are also maintained minimum. Experimental results show that the node selection mechanisms exhibit faster processing and involve low complexities. The proposed model avoids overutilization or underutilization of servers, hence making the system robust. The proposed model ensures equal distribution of load during clustering of Authentication Servers.

The MoClo-IdM framework consists of three players – the user, mobile network and the Cloud Service Provider (CSP). The IdM is located in the MobiCloud Environment which holds the Identity as a Service (IdaaS) that provides three mechanisms, namely Key Based Mutual Authentication (KBMA), Pattern Based User Authentication (PBUA) and Optimized Role Based User Authorization (ORBUA). The below fig 2 shows the workflow of the MoClo-IdM framework.

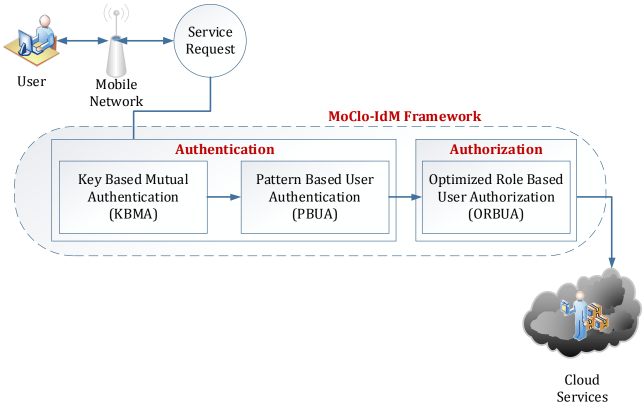
User
Mobile Network
Service Request
MoClo-IdM Framework
Authentication
Authorization
Key Based Mutual Authentication (KBMA)
Pattern Based User Authentication (PBUA)
Optimized Role Based User Authorization (ORBUA)
Cloud Services

Fig. 2 Workflow of MoClo-IdM Framework

Initially, the MobiCloud users' request for accessing the cloud services or resources. The IdM server process the request and provides the IdM services (authorization and authorization). As the first process, KBMA will be performed. KBMA is to authenticate the entities involved in accessing the cloud services. Here, the entities are the mobile devices and CSP. Two processes take place, namely; CSP authenticating device and device authenticating CSP.

After completing the KBMA, PBUA is performed to identify and authenticate the users in MobiCloud environment. The users are provided with the dynamic patterns. The dynamic patterns are matched using the pattern matching techniques. ORBUA will be performed after completing the two authentication processes. ORBUA is an effective communication technique to access cloud resources and provides security. All these three mechanisms are given as a service called Identity as a Service (IdaaS). The IdaaS is handled and given by the CSPs like other services (i.e. SaaS, IaaS, STaaS, AaaS, etc.). The user is allowed to access the cloud resources only after completing all the three processes listed in IdaaS.

4. Conclusion

The Proposed Framework, MoClo-IdM is developed to provide secure data access to the users in MobiCloud environment. MoClo-IdM consists of three different mechanisms, namely KBMA, PBUA and ORBUA. First two mechanisms; KBMA and PBUA are to authenticate the entities and the users respectively. Finally, ORBUA is proposed to authorize effectively the user for accessing the cloud resources. These three mechanisms are proposed to prevent man-in-the-middle attack, masquerading attack, password guessing attack and shoulder surfing attack. This framework also reduces the complexity and waiting time of the user. Further, incorporating game theoretic techniques to identify cluster heads will also provide an effective mechanism for identifying the best nodes.

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”, 7th International Symposium on Service-Oriented System Engineering, IEEE, 2013, ISSN: 978-0-7695, pp. 442- 453.

[2] Alizadeh Mojtaba, Saeid Abolfazli, Mazdak Zamani, Sabariah Baharun, Kouichi Sakurai, “Authentication in mobile cloud computing: A survey”, Future Generation Computer Systems, Elsevier, Volume 76, Issue 8, 2015, pp. 1-22.

[3] S. Xiao, W. Gong, Mobility can help: protect user identity with dynamic credential, In Proceedings of 11th International Conference on Mobile Data Management (MDM), IEEE, 2010, pp. 378–380.

[4] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L.B. Othmane, L. Lilien, “An Entity-centric Approach for Privacy and Identity Management in Cloud Computing”, In Proceedings of 29th IEEE Symposium on Reliable Distributed Systems, IEEE, 2010, ISSN: 1060-9857, pp. 177–183.

[5] M. Leandro, T. Nascimento, D. Santos, M. Westphall, C. Westphall, “Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments using Shibboleth”, In Proceedings of 11th International Conference on Network (ICN), Elsevier, 2012, pp. 88–93.

[6] “Oauth and Openid”, http://thenextweb.com/socialmedia /2010/07/17/oauth-and-openid-authentication-vulnerable-to-timing-attack/#!q0tFt (Accessed on 10.01.14).

[7] R. Guerrero, P. Cabarcos, F. Mendoza, D. Diaz-Sanchez, “Trust-aware Federated IdM in Consumer Cloud Computing”, In Proceedings of the International Conference on Consumer Electronics (ICCE), IEEE, 2012, ISSN: 2158-3994, pp. 53–54.

[8] Jin Yu, Chuan Tian, Heng He, Fan Wang, “A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing”, 5th International Conference on Big Data and Cloud Computing (BDCloud), IEEE, 2015, DOI: 10.1109/BDCloud.2015.57, pp.172-179.

[9] Tim Andreson, “OpenID Still Open to Abuse”, http://www.computing.co.uk/ctg/opinion/1824215/openid -abuse (Accessed on 10.01.14).

[10] Cecil DA, Arockiam l. Key Based Mutual Authentication (KBMA) mechanism for secured Access in MobiCloud environment. MATEC Web of Conferences, EDP Sciences; 2016. p. 1–5.

[11] Donald, A. Cecil, and L. Arockiam. "PBUA: A Dynamic User Authentication Mechanism for Secure MobiCloud Environment." Indian Journal of Science and Technology 9.35 (2016).

A. Cecil Donald received his Master’s in Software Engineering from Anna University, Chennai, India. He has one year experience in IT industry as a Software Developer. Currently, he is a Doctoral Research Scholar in Computer Science, St. Joseph’s College, Tiruchirappalli affiliated to Bharathidasan University, India. His main area of research is Mobile Cloud Computing. He has published 11 papers in the refereed International Journals and presented two research papers in the International Conferences. He has attended 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, Tiruchirappalli, Tamil Nadu, India. He has 27 years of experience in teaching and 19 years of experience in research. He has published more than 285 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 is also the Member of IEEE, Madras Section. 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 2012-13 and also the “Best Teacher in College” award for the year 2013 & 2014.