Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption

[(1)]R.Surendiran,
Research Scholar,
Dept of MCA, Computer Center,
Madurai KamarajUniversity,Madurai.

[(2)]Dr.K.Alagarsamy,
Associate Professor
Dept of MCA, Computer Center,
Madurai KamarajUniversity, Madurai.

***Abstract*—Now a days the mobile computing technology is emerging to provide security and increasing the scalability. The data of mobile users are send through the wireless medium there may be chances for attackers to intruding to steal the data. Security is an important and challenging issue in mobile computing environment. To increasing the security and availability of data in efficient manner we need a cloud based mobile communication. This paper proposes the access control enforcement technique with two layer of encryption to increase the security of user data in mobile cloud.**

Keywords— Cloud computing, ABE encryption, mobile computing, Access control, Key generation

I.INTRODUCTION

Mobile communication is playing an important role in most of the applications of our daily life, it allows users to access their data where ever they are. As technology increases the mobile computing has some of the important issues such as scalability, availability, mobility and security. Depends on the mobility of the mobile device the device must adopt its connection as per the mobility area. The cloud computing is a booming technology to store and retrieving the data via internet in secure and effective manner. It act as globalized data storage, we can access our data anytime anywhere through the online in secure manner. The cloud not only contains the data and also it contains applications and provides some services to the clients through the internet. The important advantages of cloud computing is extensibility, scalability and virtualization. The term mobile cloud computing is the combination of both the cloud computing and mobile network which provides data storage and data processing on the cloud environment. The main challenges behind the mobile cloud computing is security, privacy, computational cost. In mobile computing scalability is one of the challenge this can be easily rectified by mobile cloud but the security is challenging task in both mobile and cloud computing. For that we need a novel approach.

II.MOBILE CLOUD COMPUTING BACKGROUND

The mobile cloud computing is a combination of mobile computing, wireless network and cloud computing. The main advantages of mobile cloud computing is it reduces the computational cost, increases the battery backup, improves reliability and security for the mobile user. With the mobile cloud computing environment the mobile applications are placed in the mobile cloud of cloud provider and this services are offered to the mobile users they can use more number of mobile application and pay money as per the usages. These mobile applications are developed by the application developers and put on the mobile cloud environment. The layers which are present in the mobile cloud computing technology are as follows

- Application layer
- Data link layer
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Network

The primary services of mobile cloud computing are Application as a service or Software as a service, Platform as a service and infrastructure as a service. With the Application services the mobile applications are run on the cloud server which are the platform independent mobile users can pay and use those application but they cannot control and configure the settings. With the platform as a service the mobile device owner can develop new applications and also they can run their applications in the cloud environment but the user only take a control only on application and data link layer. With the infrastructure as a service the mobile users can have a control on application layer to operating system layer; they can install and run operating system.

Fig.1 Architecture of mobile cloud computing (MCC)

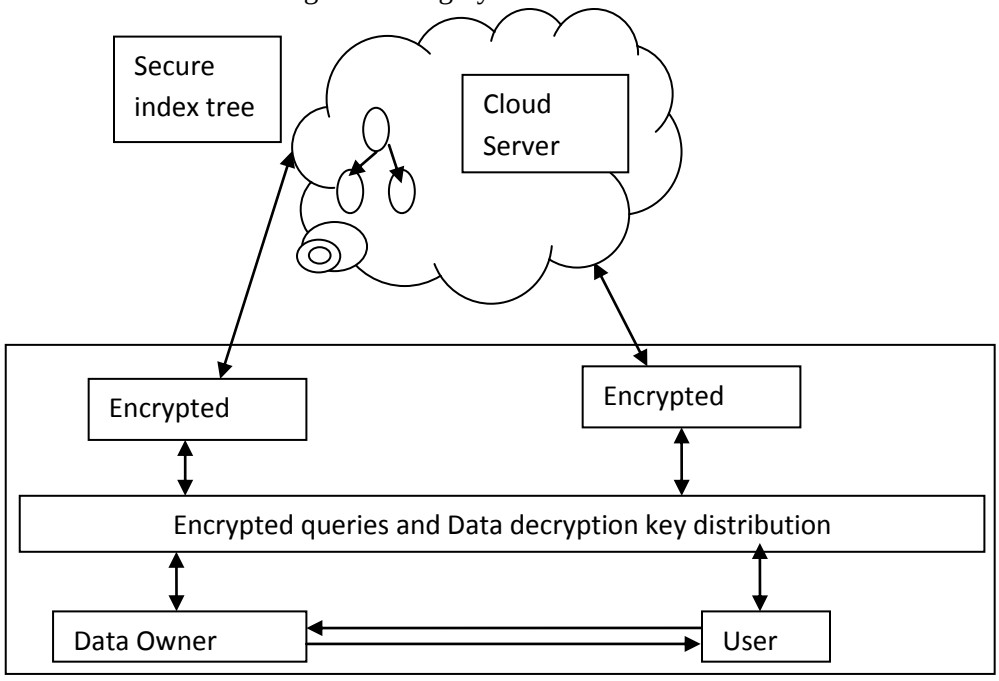
The mobile devices are connected with their corresponding base station to get the services which are offered by service provider. The services provided to the mobile user as per their information which are stored in the Home Agent

(HA). The n the control unit will send the request to the cloud server via internet, and then the services are delivered to the mobile users.

III. EXISTING SYTEM

With the mobile cloud computing all the applications and data are stored on the cloud, before uploading the data and applications in to the cloud the owner need to enforce the access control permissions by encrypting the information with certain set of attributes. So that this kind of system takes more time to computation of access control policy there is more computational overhead to the owner of data. These systems consist of data owner, identity provider, cloud and users. The identity provider provides the identity attributes to the user to access their information on the mobile cloud. Then the user requests the owner to issue the private key. By using the private key the user going to derive their access control policies.

Fig .2 Existing System Architecture



IV. PROPOSED SYTEM

In this proposed system implementing the Attribute based two layer encryption is used for providing security to access mobile cloud.

The mobile applications are placed in the mobile cloud server which is accessed by the mobile user of different mobile platform. The mobile user must pay for their use of services which is provided by the service provider. Here the major problem is resource and money paid

for the resource, if the service provided to your device is hacked by some intruder you must need to pay the money for that without using the service. So that this paper proposes the Attribute based encryption (ABE) which provides most effective security and also encryption based on the user attributes.

A. Algorithm

1. Developing mobile application

2. Setting up the access control policies

3. Setting the attributes for accessing mobile application

4. Encrypting the access control policies with application

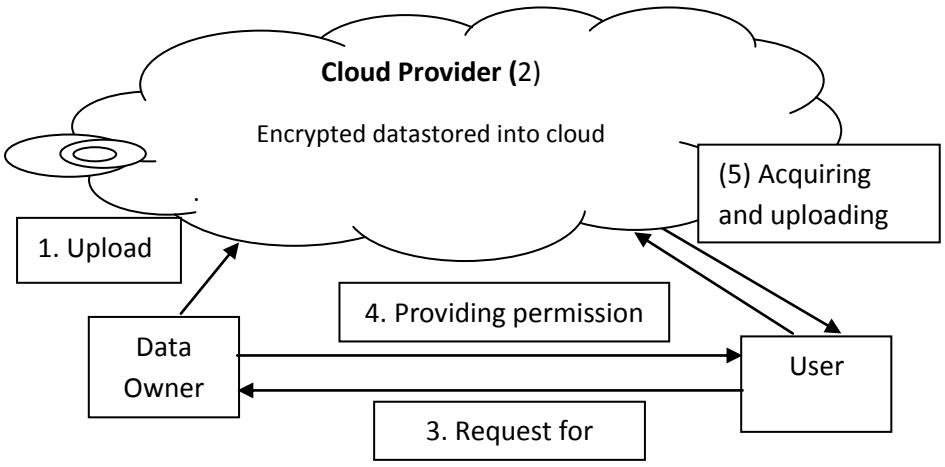
5. Uploading mobile application into cloud server

6. Enforcing secondary access control over encrypted application.

B. Attribute Based Encryption Scheme

Sahai and Waters introduces the Attribute based encryption scheme which uses the users attributes to enforcing the access control as well as encryption. The data and other information which are uploaded in to the cloud are encrypted with set of attributes of the users. While accessing the data and other services of mobile cloud the user must satisfies at least two or three attributes then only the user can access their data as well as other services. During the transfer of data and services one unique key is distributed to the users to decrypt their access policy. If the attributes are satisfied then the user can use their key to decrypt their data.

Fig.3 Proposed System Architecture



Consider the following scenario let take a three mobile users on same service provider, the mobile applications are placed on the cloud server. The service need by the mobile user must send a request through the web browser to access their applications on the server. If the request is accepted by the service provider then the cloud will check the identities of the user such as IMEI number, PIN number, port number etc, if the user satisfies some of the attributes like role, name, type of service etc, then the cloud will ask the permission network access then the user will access the services of mobile cloud. The attributes of the users are already registered in the Home Agent (HA); the control system of the base station will connect to the cloud to check certain set of attributes.

C. Two Layer Encryption Scheme

The existing approach of single layer encryption the owner of application need to set the access control policy and encrypt these access policies with set of attributes of the users and uploaded to the third party cloud storage. The main disadvantage of single layer encryption is; if the owners want to change the access control policy then the owner needs to download the application from the cloud storage and change the certain access control policies and again need to encrypt the application with access control and uploaded in to the cloud storage.

With the two layers encryption method the encryption is made on the owner side as well as mobile cloud environment. The application owner performs a encryption with some set of access control policies and then upload to the mobile cloud server then the server itself will enforce the certain set of attributes by decomposes the already encrypted attributes. The whole access control policy is divided in to two sub policies and recombining the policies to get an original policies. The mobile users need to decrypt two times to access the applications on the mobile cloud server.

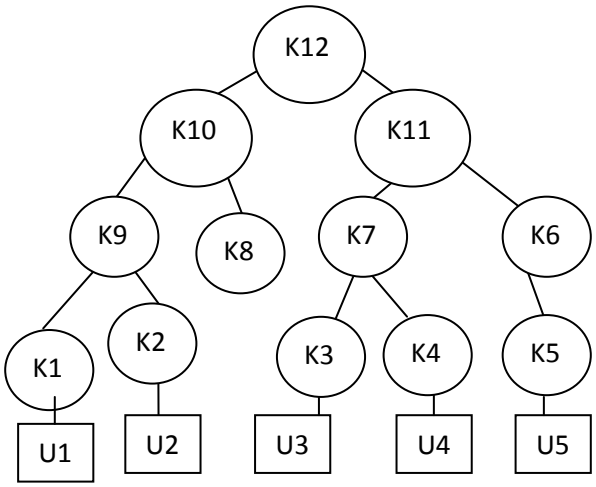
Consider the policy which are enforced to the given user (A1^A2) v (A1^A3) this policy is then divided in to two sub-policies like A1 and A2vA3. The policy A1 is enforced by the data owner by encrypted format and uploaded to the mobile cloud server with delegated access policies. The server implements another set of policy A2vA3 and encrypt the access policy over the owner encrypted policies. The mobile users need to decrypt two times to get an original access control policy and to access on their application. To decrypt the access policy the users need to request the key to the service provider then only they can decrypt the access policies and access their data and applications on the cloud.

D. Group Key Generation

The key generation is the most important part of this approach because the key

is used to decrypt the access control policies. Let take a graph which contains four groups G1, G2, G3 and G4 each group have different weight. First determine the maximum weighted node group from the tree and then choose any one randomly by any type of algorithm. In step2 add a one bit on each node groups and update the tree by put values on the edges as l and remove the edges which weight is 0.

Fig.4 Key Generation Tree before Iteration



V. PERFORMANCE EVALUATION

The multilayer attribute based encryption scheme provides higher level of security and also provides some flexibility to the application developers.

Developer: The application developer can delegate their access control policy to the cloud server no need to set a full access control policy. And also no need to download and decrypt the application, if any changes in the access control just delegating to the cloud the cloud itself enforce the access policies.

Data Owner: The data owner can delegate the access control policies to the cloud server, no need to encrypt the access control policies in the owner side. The cloud will enforce the fine-grained access control which is delegated by the application owner. Some of the access control policies are Memory usage, Uploading and Downloading limit, Expiry date for the applications usage, Session time etc.

Mobile Users: The mobile users just request their private key to decrypt the access control policies. But the decryption process is not performed on the user's device; it performed on the cloud itself. So that the user performs less computational process; the user device has less CPU processor, low memory and bandwidth.

Fig.5 Performance of Existing VS Proposed based on Time (sec)

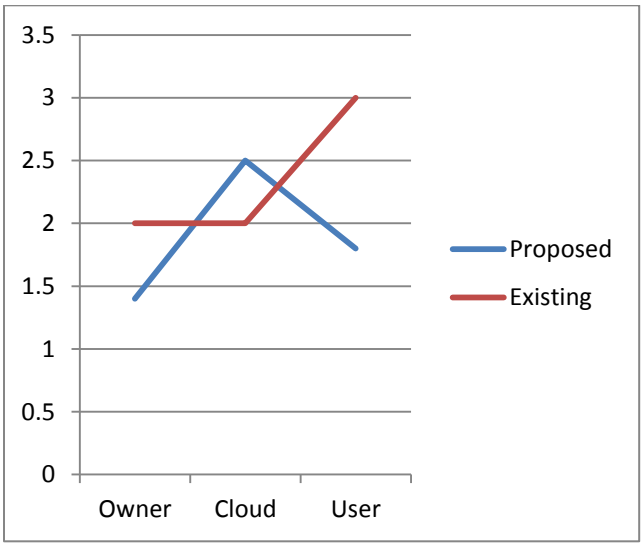


Table.1 Performance of Existing Vs Proposed

Approach	Key length	Owner In(sec)	Cloud In(sec)	User In(sec)
Existing	256bit	2sec	2sec	3sec
Proposed	128bit	1.4sec	2.5sec	1.7sec

VI. CONCLUSION

The cloud computing is the most emerging technology to manage the huge amount of data and other services. This technology is well suited for the mobile computing purpose so that the mobile cloud is introduced by combining these two environments. The most important issues taken in this paper is security and scalability. To compromise these two things we need a new kind of approach to protect the information from the intruders. The mobile cloud is served on the basis of pay on their usage so that this process involves the money transaction we need to provide more security options to the mobile users.

This paper proposes the Attribute Based Two Layer Encryption scheme which the data and other services are verified through the set of identity attributes. The existing approach uses only single layer encryption which is not a sufficient security for the money transaction oriented process. This proposed system will provide more confidentiality as well as security to the mobile cloud users.

REFERENCES

[1] S. Xinogalos, K. E. Psannis, and A. Sifaleras, "Recent advances delivered by HTML 5 in mobile cloud computing applications: a survey," in *Proc. the Fifth Balkan Conference in Informatics*, 2012, pp. 199-204.

[2] Khan, M. Othman, S. Madani, and S. Khan, "A survey of mobile cloudcomputing application models," *IEEE Communications Surveys &Tutorials*, issue 99, 2013.

[3] Peter Mell, Tim Grance, "The NIST definition of Cloud Computing", v15.

[4] Sean Marston, Zhi Li, SubhajyotiBandyopadhyay, Juheng Zhang, AnandGhalsasi, "Cloud Computing – The business perspective", Decision Support Systems, Volume 51, Issue 1, Pages 176-189, 2011

[5] Han Qi, Abdullah Gani, "Research on Mobile Cloud Computing: Review,Trend and Perspectives" in Proceedings of the Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP), IEEE, Pages 195-202, 2012.

[6] M. Nabeel, N. Shang, and E. Bertino. Privacy preserving policy based content sharing in public clouds.*IEEE Transactions on Knowledge and Data Engineering*, 99, 2012.

[7] OpenID. http://openid.net/ [Last accessed: Oct. 14, 2012].

[8] T. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *CRYPTO 1991:Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, pages129–140, 1992.

[9] N. Shang, M. Nabeel, F. Paci, and E. Bertino.A privacy-preserving approach to policy-based contentdissemination. In *ICDE 2010: Proceedings of the 2010 IEEE 26th International Conference on DataEngineering*, 2010.

[10] S. Yu, C. Wang, K. Ren, and W. Lou. Attribute based data sharing with attribute revocation. In *ASIACCS2010: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*,pages 261–270, 2010.