TEST Engineering & Management

November/December 2020
ISSN: 0193-4120 Page No. 245-251

Fine Grained Access Control of Data in Mobile Cloud Computing

Gurpreet Kaur[1], Mahendra Kumar[2]

[1,2]Guru Kashi University, Talwandi Sabo

Article Info
Volume 83
Page Number: 245-251
Publication Issue:
November/December 2020

Article History
Article Received*: 25 October 2020*
Revised*: 22 November 2020*
Accepted*: 10 December 2020*
Publication*: 31 December 2020*

Abstract
With the increasing number of mobile applications and the popularity of cloud computing, mobile cloud computing (MCC) attracts great attention in recent years. While using the cloud storage services on resource constraint mobile device, the mobile user needs to ensure the confidentiality of the critical data before uploading on the cloud storage. This paper focused on analysis of five different techniquesType-Based Proxy Re-Encryption, Coding-Based Scheme,Decentralized Attribute Based Encryption (ABE), Ciphertext Policy Attribute-Based Encryption (CP-ABE), A Multi-Authority CP-ABE Scheme. These method contain some issue and drawbacks. To overcome some issue, this paper has proposed Fine-Grained Access Control using Tree Structure scheme.By security analysis and performance evaluation, the proposed scheme is proved to besecure as well as efficient in mobile cloud computing.
Keywords: *Mobile cloud, CP-ABE.*

I) INTRODUCTION

MCC is a service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional [1]. The main objectives of the mobilecloud computing are to increase the processing/storagecapabilities of the mobile device and reduce the energyconsumption while executing the computationally intensivejobs [2].To achieve the aforementioned objectives, mobile users offload processing intensive and storage demanding portion of mobile application from resource constraint mobile device to resource enriched cloud [3]. The offloading of the processing intensive and storage demanding portion(s) of mobile application enhances the capabilities of mobile devices in term of processing, storage, and battery [4].In order to ensure the confidential of data as well as the access control, lots of studies focus on combining mobile cloud computing and CP -ABE [5].

This paper discuss five scheme for the data access in mobile cloud computing such as Type-Based Proxy Re-Encryption, Coding-Based Scheme,Decentralized Attribute Based Encryption (ABE), Ciphertext Policy Attribute-Based Encryption (CP-ABE), A Multi-Authority CP-ABE Scheme..

But these method also have some problem so to overcome that Fine-Grained Access Control using Tree Structure scheme is proposed in this paper.

II) BACKGROUND

In the mobile cloud computing Fine-Grained Access Control using Tree Structure schemes are used. A new type-based proxy re-encryption to design a secure and efficient data distribution system in MCC, which provides data privacy, data integrity, data authentication, and flexible data distribution with access control. Compared to traditional cloud-based data storage systems, this system is a lightweight and easily deployable solution for mobile users in MCC since no trusted third parties are involved and each mobile user only has to keep short secret keys consisting of three group elements for all cryptographic operations [1].The resource limitation of mobile devices restricts mobile users for executing complex security operations using computational power of mobile devices. To make security schemes suitable for mobile devices, large volume of existing security schemes execute complex security operations remotely on cloud or trusted third party .The Coding based scheme uses matrix multiplication and cryptographic hash function for providing confidentiality and integrity services to mobile users in cloud environment.[2].A decentralized attribute based encryption (ABE) scheme with fast encryption, outsourced decryption and user revocation. The proposed scheme is very specific to the context of mobile cloud as the storage of encrypted data and the partial decryption of ciphertexts are dependent on the cloud and users with mobile devices can upload data to the cloud or access data from it by incurring very little cost for encryption and decryption respectively [3].The Ciphertext Policy Attribute-Based Encryption (CP-ABE), has been used for realizing fine-grained access control on encrypted data stored in MCC. However, the computational overhead of encryption and decryption grow with the complexity of the access policy. Thus, maintaining data security as well as efficiency of data processing in MCC are important [4]. The multi-authority CPABE scheme is improve security of implementation supports a Certificate Authority, independent of Cloud Service Provider, and signed Revocation Lists. The prototype can interoperate with existing cloud storage via API. The computational overhead is distributed among a large number of users, instead of assigning them to any particular party[5].

This paper introduces five data access scheme Type-Based Proxy Re-Encryption, Coding-Based Scheme,Decentralized Attribute Based Encryption (ABE), Ciphertext Policy Attribute-Based Encryption (CP-ABE), A Multi-Authority CP-ABE Scheme.

The paper is organised as follows:

Section I Introduction.**Section II** discusses Background. **Section III** discusses previous work.

Section IV discusses existing methodologies.

Section V discusses attributes and parameters and how these are affected on mobile cloud computing. **Section VI** proposed method and outcome result possible. Finally **Section VIII** Conclude this paper.

III) PREVIOUS WORK DONE

Jiang Zhang et al (2017)[1]has proposedType-Based Proxy Re-Encryptionwhich provides data privacy, data integrity, data authentication, and flexible data distribution with access control.

Abdul Nasir Khan et al (2013)[2] has proposed Coding-Based Schemefor for providing

confidentiality and integrity services to mobile users in cloud environment.

Sourya Joyee Deet al (2017) [3] has proposedDecentralized Attribute Based Encryption (ABE)specific to the context of mobile cloud as the storage of encrypted data and the partial decryption of ciphertexts are dependent on the cloud and users with mobile devices can upload data to the cloud or access data from it by incurring very little cost for encryption and decryption respectively.

Jing Li1et al (2017) [4] has proposedThe Ciphertext Policy Attribute-Based Encryption (CP-ABE)scheme it has been used for realizing fine-grained access control on encrypted data stored in MCC.

Ilka Aet al (2017)[5] has proposed cloudlets scheme which introduces a middle layer sitting between mobile devices and their cloud infrastructure. The multi-authority CPABE scheme is improve security of implementation supports a Certificate Authority, independent of Cloud Service Provider, and signed Revocation Lists.

IV) EXISTING METHODOLOGIES

For secure data access in mobile cloud computing Type-Based Proxy Re-Encryption, Coding-Based Scheme,Decentralized Attribute Based Encryption (ABE), Ciphertext Policy Attribute-Based Encryption (CP-ABE), A Multi-Authority CP-ABE scheme are used.

A] Type-Based Proxy Re-Encryption:

Type-Based Proxy Re-Encryption which allows a mobile user with a single secret key to keep the data privacy, and flexibly share his data with friends under permission.Figure 1 Shows System model of data distribution system**.**There are three main network entities in data distribution system, namely, the cloud, the data owner and the data consumer.

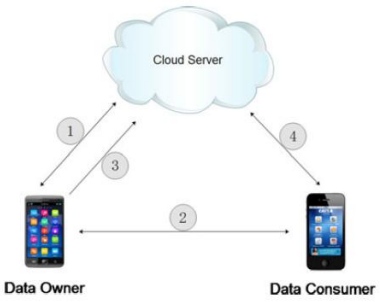


Figure 1: System model of data distribution system

The data owner is a mobile user who stores his private data in the cloud (by different categories), andallows the data consumer to access his private data (of some category) from the cloud.The cloud is an entity who provides storage services and is responsible to help the data owner to distributethe private data (belonging to some particular category) to the data consumer.The data consumer is an entity who first gets data access permission (of some data category) from thedata owner (and this only happens once per data category), and then access the data owner's private data. from the cloud.[1].

B] Coding-Based Scheme:

Coding-Based SchemeCoS uses matrix multiplication and cryptographic hash function for providing confidentiality and integrity services to mobile users in cloud environment. For uploading, the mobile user divides the file into'd' parts, each part is represented in the form of matrix having 't' rows of size 'n' bits. The mobile user must provide a password to generate the coding vector.The coding vector is generated by performing recursive hash function on concatenation of password, file name, and file size[2].

November/December 2020
ISSN: 0193-4120 Page No. 245-251

C]Decentralized Attribute Based Encryption (ABE) Scheme:

Decentralized Attribute Based Encryption (ABE)this scheme propose a decentralized access control mechanism based on a multi-authority CPABE scheme with fast encryption and outsourced decryption. The first scheme that significantly reduces computation overhead from both data owners and data users in the decentralized setting. The properties of decentralization, online/offline mode of encryption and outsourced decryption make a CPABE scheme suitable for practical applications.The system figure 2 shows The Data Owner (DO) is an entity that owns data and uploads it to cloud storage after encrypting it

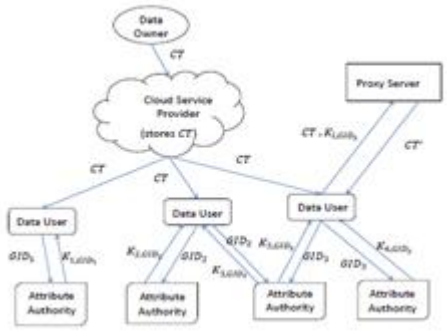


Figure2: System Model

Data owners do not want the CSP to learn anything about their data and allows access to the data users whose attributes satisfy a given policy. Data owners may need to use resource-constrained devices (e.g., mobile phones, sensors, smartcards) to perform encryption on their data. All devices used by DO are assumed trusted. The Cloud Service Provider (CSP) provides storage facilities for data belonging to data owners. The CSP is honest-but-curious. The CSP can try to find out information from the data stored in it but does not modified or deletes data. Data Users (DU) want to access data outsourced by the DO to the CSP. They can access this data if they satisfy a given policy. There are more than one Attribute Authorities (AA) controlling different user attributes and generate the public key and decryption key corresponding to these attributes[3].

D] Ciphertext Policy Attribute-Based Encryption (CP-ABE) Scheme:

Ciphertext Policy Attribute-Based Encryption (CP-ABE) CP-ABE which can dramatically enhance data encryption efficiency without loss of data security and data privacy**.** The proposed scheme has an efficient encryption method, especially when users require to repeatedly encrypt the messages under the same access structure. The CPABE scheme has additionally apply verifiable outsourced decryption to scheme. The CPABEhas shown the security analysis and provide a detailed performance evaluation to demonstrate the advantages of scheme[4].

E] A Multi-Authority CP-ABE scheme:

A Multi-Authority CP-ABE is suitable for the implementation of ABAC for cloud storage. The illustration of the proposed scheme is shown in Figure 3.This identified the following main system components-

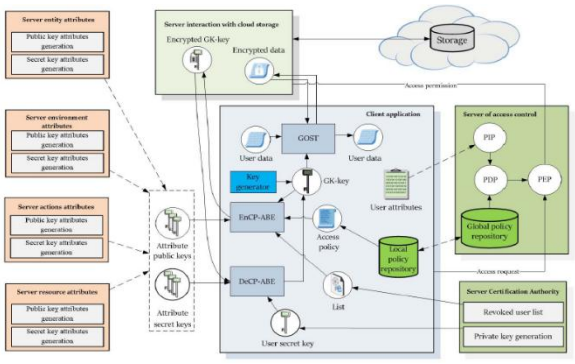


Figure 3: Main system components CPABE

ABAC Servers, including server resource attributes, server entity attributes, server environment attributes,

November/December 2020
ISSN: 0193-4120 Page No. 245-251

and server actions attributes, Certification Authority

Server working as a gateway for interaction with cloud storage, access control serverclient's application [5].

V) ANALYSIS AND DISCUSSION

Type-Based Proxy Re-Encryption this method propose a practical data distribution system in mobile cloud computing, which does not involve any trusted third party and provides several useful properties including data privacy, data integrity, data authentication, dynamic data modifications and deletions, as well as fine-grained access control[1].

Coding-Based Scheme CoS uses matrix multiplication and cryptographic hash function for providing confidentiality and integrity services to mobile users in cloud environment [2]

Decentralized Attribute Based Encryption (ABE) proposed scheme compare the performances of the encryption and decryption algorithm and the cipher text size.It combines the useful properties of decentralization, fast encryption, outsourced decryption and user revocation[3].

Ciphertext Policy Attribute-Based Encryption (CP-ABE),an efficient encryption scheme which can not only guarantee secure data access, but also reduce overhead both on DO and DR. The security analysis shows that the proposed scheme can meet the security requirement. The evaluations show the advantages on the efficiency of data encryption[4].

A Multi-Authority CP-ABE Scheme on the basis of the system is multi-authority attribute-based encryption scheme. The progress of cloud technologies makes possible efficient and secure data storage. However access control is very important to make cloud storage secure. Existing solutions provide a versatility access control system [5].

Scheme	Advantages	Disadvantages
Type-Based Proxy Re-Encryption	Data privacy, Data integrity, Data authentication, Dynamic data modifications	Lazy revocation on the access permission
Coding-Based Scheme	Confidentiality and Integrity services	Resource constraint mobile devices
Decentralized Attribute Based Encryption (ABE)	Enhance data encryption efficiency	System efficiency is a challenging issue
Ciphertext Policy Attribute-Based Encryption (CP-ABE)	CP-ABE is suitable for the implementation of ABAC for cloud storage.	Not Flexible.
A Multi-Authority CP-ABE Scheme	easier for maintenance	Revocation is a particularly difficult problem for CP-ABE. .

TABLE 1: Comparisons between different Schemes

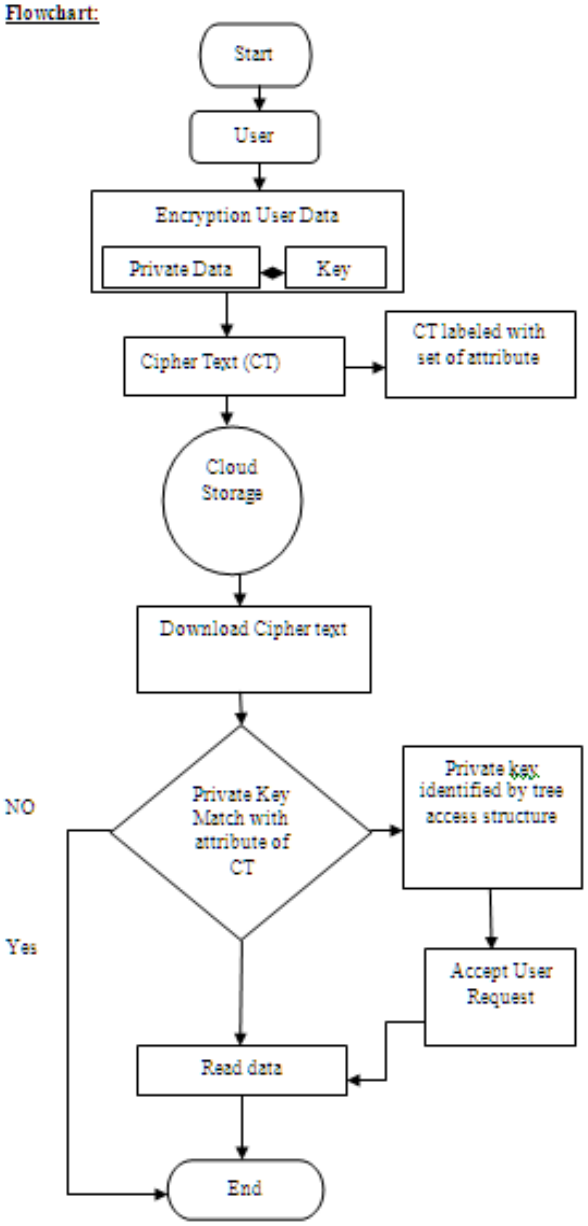
November/December 2020
ISSN: 0193-4120 Page No. 245-251

PROPOSED METHODOLOGY

Fine-Grained Access Control using Tree Structure:

This proposed scheme isa declarative way to define access rights, task assignments, recipients and content in information systems.Fine-grained access control means granting access right of individual users. This scheme define the access policy based on attribute set, and cipher text is labelled with this attribute set and private key are embedded with access structure, to decrypt the Cipher text system will be able to match the access structure with private key of user. This scheme define the access policy on AND/OR gate tree structure. Different pieces of data are decrypted by different users according to access structure is the main advantage of this scheme.The tree structure is secure and efficient access mechanism used to access the user data and match private key.

Flowchart:



VII) OUTCOME AND POSSIBLE RESULT

By security analysis and performance evaluation, the proposed scheme is proved to be secure as well as efficient for the accessing data and efficient access control of data in security environment in mobile cloud computing.

VIII)CONCLUSION

This paper focused on the study of five different schemes these areType-Based Proxy Re-Encryption, Coding-Based

Scheme,Decentralized Attribute Based Encryption (ABE), Cipher text Policy Attribute-Based Encryption (CP-ABE), A Multi-Authority CP-ABE Scheme. The proposed scheme is provide access rights to the user and high data security in Mobile Cloud Computing.

IX) FUTURE SCOPE

From observation, the scope is planned to be studied in future work that proposed scheme can be used in any high end data access and security system.

REFERENCES

1. YANG Kan, JIA Xiaohua, Expressive, Efficient, and
2. Revocable Data Access Control for Multi-Authority-
3. Cloud Storage [J], IEEE Trans. Parallel and Distributed Systems, 2014.
4. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, “Towards Secure Mobile Cloud Computing: A Survey,” Future Generation Computer Systems, vol. 29, pp. 1278-1299, July 2013.
5. N. Balani and S. Ruj. Temporal access control with user revocation for cloud data. In 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014, Beijing, China, September 24-26, 2014, pages 336–343, 2014.
6. A N KhanML Mat KiahSU KhanSA Madani, “Towards secure mobile cloud computing: A survey”, Future Generation Computer
7. Systems, vol. 29, no. 5, pp. 1278-1299, July. 2013.Mining. New York, NY,USA: Springer, 2012.
8. Horvath M. Attribute-Based Encryption Optimized for Cloud Computing. In SOFSEM 2015.