ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.9

Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing

Shreyas. KS[1], Prof. Divakar. HR[2]
PG Scholar[1], Professor[2]
Department of MCA
PES College of Engineering, Mandya, India

Abstract:
With the development of cloud computing, outsourcing data to cloud server attracts lots of attentions. To guarantee the security and achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used in cloud storage system. However, user revocation is the primary issue in ABE schemes. In this article, we provide a ciphertext-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys. Notably, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. We prove the security of our scheme under the divisible computation Diffie-Hellman (DCDH) assumption. The result of our experiment shows computation cost for local devices is relatively low and can be constant. Our scheme is suitable for resource constrained devices.

I. INTRODUCTION

In this project, we provide a cipher text-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys.

II. OBJECTIVE

Security issues are main obstacles for wide application of cloud computing. To achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used. However, user revocation is the primary issue in ABE schemes. We need efficient user revocation for cloud storage system. At the same time heavy computation cost should not spoil the application performance. The system should with stand collusion attack performed by revoked users cooperating with existing users. The system should be suitable for resource constrained devices also.

III. SCOPE

- It provides data security and achieves flexible &fine-grained file access control .
- It handles revocation efficiently.
- It is collusion attack proof system.
- It fulfills the client's requirement cost effectively.
- It is high in performance.
- It is robust and reliable system

IV. SYSTEM ARCHITECTURE:

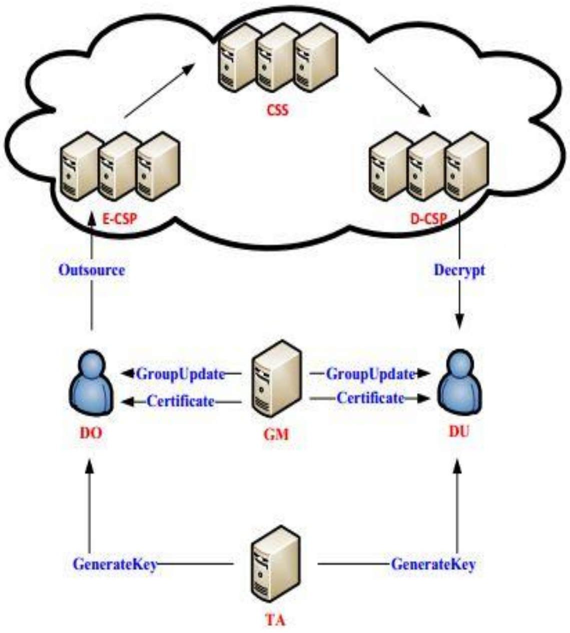

Figure.2. System Architecture

V. EXISTING SYSTEM:

- Boldyreva et al. presented an IBE scheme with efficient revocation, which is also suitable for KP-ABE. Nevertheless, it is not clear whether their scheme is suitable for CP-ABE.

- Yu et al. provided an attribute based data sharing scheme with attribute revocation ability. This scheme was proved to be secure against chosen plaintext attacks (CPA) based on DBDH assumption. However, the length of cipher text and user's private key are proportional to the number of attributes in the attribute universe.

- Yu et al. designed a KP-ABE scheme with fine-grained data access control. This scheme requires that the root node in the access tree is an AND gate and one child is a leaf node which is associated with the dummy attribute.

VI. DISADVANTAGES OF EXISTING SYSTEM:

- It is expensive in communication and computation cost for users.

- Unfortunately, ABE scheme requires high computation overhead during performing encryption and decryption operations. This defect becomes more severe for lightweight devices due to their constrained computing resources.

- There is a major limitation to single-authority ABE as in IBE. Namely, each user authenticates him to the authority, proves that he has a certain attribute set, and then receives secret key associated with each of those attributes. Thus, the authority must be trusted to monitor all the attributes. It is unreasonable in practice and cumbersome for authority.

VII. PROPOSED SYSTEM:

- In this system, we focus on designing a CP-ABE scheme with efficient user revocation for cloud storage system.

- We aim to model collusion attack performed by revoked users cooperating with existing users.

- Furthermore, we construct an efficient user revocation CP-ABE scheme through improving the existing scheme and prove our scheme is CPA secure under the selective model.

- To solve existing security issue, we embed a certificate into each user's private key. In this way, each user's group secret key is different from others and bound together with his private key associated with attributes.

- To reduce users' computation burdens, we introduce two cloud service providers named encryption-cloud service provider (E-CSP) and decryption-cloud service provider (D-CSP).

- The duty of E-CSP is to perform outsourced encryption operation and D-CSP is to perform outsourced decryption operation.

VIII. ADVANTAGES OF PROPOSED SYSTEM:

- Reduce the heavy computation burden on users.

- We outsource most of computation load to E-CSP and D-CSP and leave very small computation cost to local devices.

- Our scheme is efficient for resource constrained devices such as mobile phones.

- Our scheme can be used in cloud storage system that requires the abilities of user revocation and fine-grained access control.

IX. IMPLEMENTATION

MODULES:

- Data Owner(DO)
- Data User(DU)
- Group Manager(GM)
- Auditor
- Cloud Storage Server(CSS)

X. MODULES DESCRIPTION:

- **Data Owner (DO):**

In this module includes the Data Owner first register his details and login. Next The Owner gives the request to Group Manager for Group Certificate. After receive the certificate DO can Upload a file to the Cloud and the file encrypted by the CP-ABE Algorithm. The Data Owner can also view the Files details and File contents in a Encrypted format. The Data Owner can only View his Group Files.

- **Data User (DU):**

In this module includes the Data User first register his details and login. Next The User gives the request to Group Manager for Group Certificate. After receive the certificate DU can View a file Details. If Data User wants to download the file means DU send the request to the Auditor for Secret Key of downloading permission. Auditor sends the Secret Key to Data User Mail id. Data User can download the file by using the Secret Key. Data User view and download his Group files only.

- **Group Manager (GM):**

In this Module Group Manager response Data Owner and Data User Group Certificate requests. Group Manager sends the Group Certificates to the DO and DU. Group Manager done the Users Revocation Process. Once the User is Revoked by GM then the user not able to access the files in the group and the user is unauthorized to login.

- **Auditor:**

In this Module the Auditor can view the Uploaded file details and Auditor response the Data Users Secret Key Requests for Downloading process. Auditor sends the Secret Key to the Data Users Mail id. Without this secret key Data User Cannot able to download the files.

- **Cloud Storage Server (CSS) :**

The Cloud Storage Server can view the Data Users and Data Owners Details.CSS can also view the File Details .and CSS view the revoked Users Details.

XI. CONCLUSION

We provided a formal definition and security model-ABE with user revocation. We also constructed a concrete CP-ABE scheme which is CPA secure based on DCDH assumption. To resist collusion attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key through combining their private keys. Additionally, we outsource operations with high computation cost to reduce the user's computation burdens. Through applying the technique of outsource, computation cost for local devices is much lower and relatively fixed. The results of our experiment show that our scheme is efficient for resource constrained devices.

XII. FUTURE ENHANCEMENT

- Better algorithm than CP-ABE can be designed to improve the performance.
- UI can be improved
- Private key can be sent to mobile phone
- Data leakage detection mechanism can be implemented
- Remote access and faster disaster recovery.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

➢	System	:	Intel 2.1 GHZ
➢	Hard Disk:		40 GB.
➢	Ram :		2GB.

SOFTWARE REQUIREMENTS:

➢	Operating system	:	Windows 7.
➢	Coding Language	:	JAVA/J2EE
➢	Tool	:	Netbeans 7.2.1
➢	Database	:	MYSQL

XIII. REFERENCE:

[1]. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," EUROCRYPT'05, LNCS, vol. 3494, pp. 457-473, 2005.

[2]. J.Bethencourt, A.Sahai and B.Waters, "Ciphertext-Policy Attribute-Based Encryption,"Proc. IEEE Symposium on Security and Privacy, pp.321-334, May 2007, doi: 10.1109/SP. 2007.11.

[3]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based En-cryption for Fine-Grained Access Control of Encrypted Data,"Proc.13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89-98, 2006, doi: 10. 1145 /1180405.1180418.

[4]. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal of Computing, vol. 32, no. 3,pp. 586-615, 2003.

[5]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation,"Proc.15th ACM conference on Computer and communications security (CCS' 08),pp. 417-426, 2008.