IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A LEAGUE KEY CONTROL USING ENCRYPTION AND DECRYPTION PROCESS IN CLOUD SERVER

[1]Pallela Kavya, [2]Keshetty Deepika,[3]Vadde Madhuri,[4]Dr.V.Anantha Krishna

[1]Student, [2]Student, [3]Student, [4]Professor

Department of Computer Science and Engineering

Sridevi Women's Engineering College ,Vattinagulapally,Gandipet,R.R.DIST-500075,India

Abstract: **Ciphertext policy attribute-based encryption (CP-ABE) is a type of cryptographic technique where we can control the access of outsourced data in the cloud. However, some drawbacks of key management obstruct the popularity of its application. One drawback in urgent need of solution is the key escrow problem. We indicate that front-end devices of clients like smartphones generally have only limited privacy protection, so if private keys are entirely held by them, clients risk key exposure that is hardly noticed but inherently existed in previous research. Here, we propose a collaborative key management protocol in CP-ABE (CKM-CP-ABE). This construction realizes distributed generation, issue and storage of private keys without adding any extra infrastructure. It also provides a fine-grained and immediate attribute revocation for key update.**

Key Terms **- Encryption,Decryption,Cloud server.**

I. INTRODUCTION

In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this project, we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. One of the most challenging issues we face in data sharing systems is the enforcement of access policies and the support of policies updates. Ciphertext policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic solution to this issue. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed.

CP-ABE is quite suitable for the construction of secure, fine-grained access control for cloud data sharing [27][28]. However, there are still a lot of open challenges concerning the practical realization of ABEs especially in terms of private key management. For large numbers of previous ABE schemes [2][3][4][5][6][7], the key authority must be completely trustworthy, as it can decrypt all the ciphertext using a generated private key without permission of its owner. This is commonly called the key escrow problem and is an inherent disadvantage that threatens user privacy. Together with the growth of mobile applications, mobile cloud services [24] [31] have been introduced as a potential trend in cloud computing. Current research work hardly notices that mobile front-end devices, such as smartphones, are far more vulnerable than servers with respect to privacy protection [20]. Thus, the vulnerability in private key protection may easily lead to the exposure of keys to unauthorized users [30]. In addition, current ABE key management schemes also require much bilinear pairing calculation, exponentiation and multiplication, especially in the decryption step [5][29]. The resulting run time may be horribly unacceptable. In this paper, we propose a novel collaborative key management protocol in ciphertext policy attribute-based encryption (CKM-CP-ABE) aiming to enhance security and efficiency of key management in cloud data sharing systems. The main contributions are summarized as follows:

1. A novel collaborative protocol is presented. With help of interaction among the key authority, a cloud server and a client who tends to access data,distributed generation, issue and storage of private keys are realized.
2. We introduce attribute groups to build the private key update algorithm. A unique attribute group key is allocated to each attribute group that contains clients who share the same attribute.
3. We indicate that not only the key escrow problem but also key exposure is threatening the confidentiality of private keys, which is hardly noticed in previous research. Compared to previous key management protocols for attribute-based data sharing systems in the cloud, our proposed protocol effectively addresses both two problems by its collaborative key management. Finally, we provide proof of security for the proposed protocol.

II. OBJECTIVES

The proposed collaborative mechanism not only solves the key escrow problem but also solves the key exposure. Meanwhile, it helps to reduce client encryption overhead. When we compare with other representative CP-ABE schemes, it demonstrates that our scheme has somewhat better performance in terms of cloud-based outsourced data sharing on mobile devices. Finally, we provide proof of security for the proposed protocol.

III. PROBLEM STATEMENT

In a collaborative key management system, the existing system faces a key escrow problem. So, we proposed a novel collaborative key management protocol in ciphertext policy attribute-based encryption (CKM-CP-ABE) scheme to overcome this key escrow problem. This novel collaborative key management protocol enhances security and efficiency of key management in cloud data sharing systems.

IV. PROPOSED SYSTEM

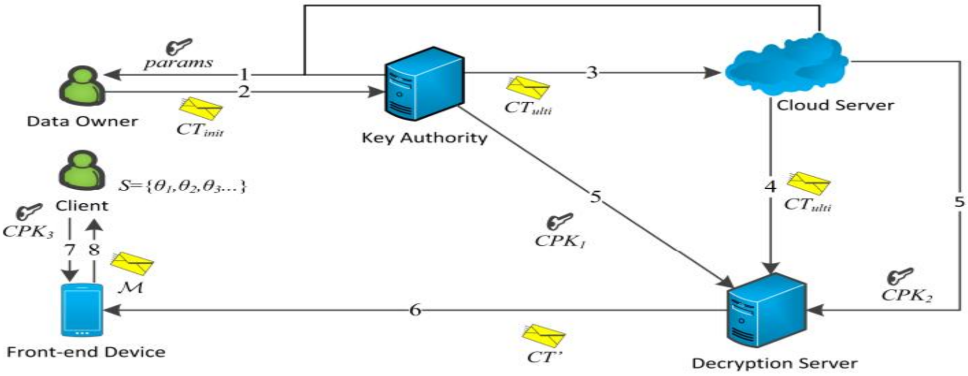
In this paper, we propose a novel collaborative key management protocol in ciphertext policy attribute-based encryption (CKM-CP-ABE) aiming to enhance security and efficiency of key management in cloud data sharing systems. With the help of interaction among the key authority, a cloud server and a client who tends to access data, distributed generation, issue and storage of private keys are realized. We introduce attribute groups to build the private key update algorithm. A unique attribute group key is allocated to each attribute group that contains clients who share the same attribute. Via updating attribute group key, a fine-grained and immediate attribute revocation is provided. The collaborative mechanism helps markedly reduce client decryption overhead by employing a decryption server to execute most of the decryption while leaving no knowledge about information to it.

V. ADVANTAGES OF PROPOSED SYSTEM:

- Secure key management is guaranteed without adding any extra physical infrastructure, which is easier to deploy compared with previous multi-authority schemes
- We indicate that not only the key escrow problem but also key exposure is threatening the confidentiality of private keys, which is hardly noticed in previous research.

VI. SYSTEM DESIGN

System Architecture



Module description:

Client

A client (CL) is a user who intends to access data in cloud storage via front-end devices. With the potential trend of mobile cloud services, mobile devices are the majority of front-end devices. If the CL's attribute set satisfies an access policy associated with ciphertext, the CL will be allowed to acquire plaintext. We assume that most mobile devices are performance-restrained, so CLs may be in danger of suffering key exposure.

Key Authority

The key authority (KA) is a vital component in the system. The KA is responsible for most calculating tasks, including key generation, key update, etc. We assume that the KA is semi-trusted in our system, meaning it is curious about the value of plaintext but has no intention of tampering with it.

Cloud Server

A cloud server (CS) is responsible for cloud storage management. All the data to be shared is in the control of the CS. We assume that any CS is semi-trusted.

Decryption Server

The decryption server (DS) has powerful computing capabilities. It undertakes and isolates most, but not all, tasks of decryption. We assume that the DS is semi-trusted and the DS access channel is insecure, because it is sufficient for CKM-CP-ABE to guarantee data security, which will be demonstrated in Section IV.

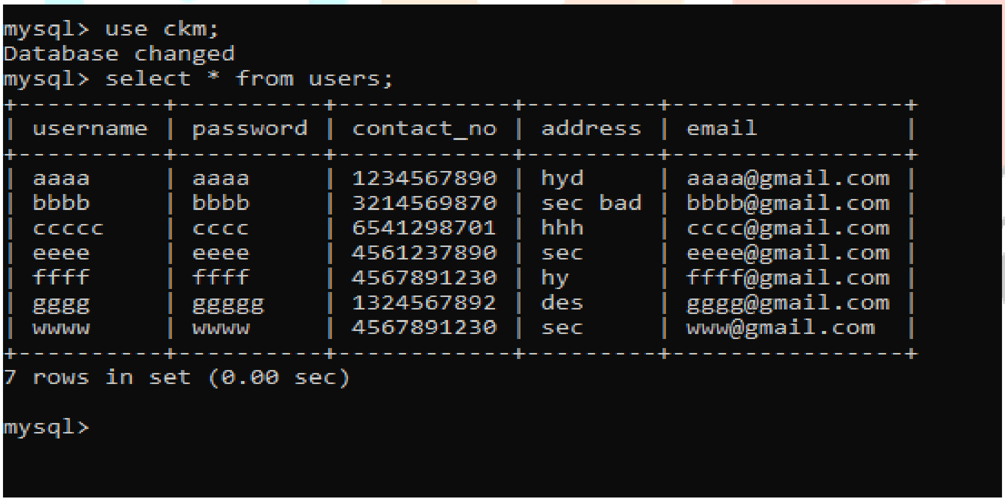
Data Owner

A data owner (DO) is an authorized user in the system that possesses data to be uploaded. DOs define their own explicit access policies so that only desirable CLs are granted permission to obtain plaintext.

VII. RESULT AND DISCUSSION

Result

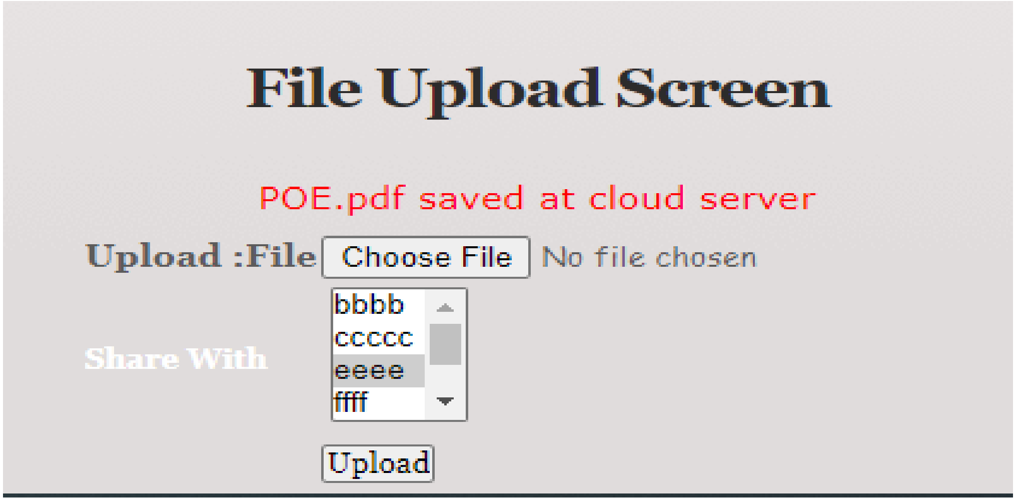
Here we are running the code to display the page, where the user can register with the required credentials. When the users register the key authority will generate a secret key for registered users. Then the user details are approved and stored which we can see in the database server.



```
mysql> use ckm;
Database changed
mysql> select * from users;
+----------+----------+------------+---------+----------------+
| username | password | contact_no | address | email          |
+----------+----------+------------+---------+----------------+
| aaaa     | aaaa     | 1234567890 | hyd     | aaaa@gmail.com |
| bbbb     | bbbb     | 3214569870 | sec bad | bbbb@gmail.com |
| ccccc    | cccc     | 6541298701 | hhh     | cccc@gmail.com |
| eeee     | eeee     | 4561237890 | sec     | eeee@gmail.com |
| ffff     | ffff     | 4567891230 | hy      | ffff@gmail.com |
| gggg     | ggggg    | 1324567892 | des     | gggg@gmail.com |
| wwww     | wwww     | 4567891230 | sec     | www@gmail.com  |
+----------+----------+------------+---------+----------------+
7 rows in set (0.00 sec)

mysql>
```

When the user or owner login and if he/she is valid then the user can upload the file and also be able to select any one registered user so that they can download to use that file.



File Upload Screen

POE.pdf saved at cloud server

Discussion

If the same data owner uploads another file with the same shared user policy then this application will not generate another key. It will form a group with the same share policy. With this we can avoid extra key generation time.

VIII. CONCLUSION AND FUTURE SCOPE

Conclusion

Ciphertext policy attribute-based encryption is a promising cryptographic technique to realize fine-grained access control in secure cloud storage.In this paper, we propose a novel league key control protocol to enhance both security and efficiency of key management in ciphertext policy attribute-based encryption for cloud data sharing.Distributed key generation, issue and storage of private keys are realized without adding any extra physical infrastructure.

Future Scope

Our future work will build on the preliminary findings in this work to develop the proposed scheme by reducing ciphertext size, encryption cost and decryption cost, which are still open problems that hinder practical application of attribute-data sharing. Considering some specific industrial scenarios such as personal health record access control, besides, the expressiveness of access policy needs enhancement as well.

IX. REFERENCE

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. EuroCrypt, 2005, pp. 457-473. [2] J. Bethencourt, A. Sahai, and B.Waters, “Ciphertext-policy attribute-based encryption,” in Proc. IEEE Symp. Secur. Privacy, 2007, pp. 321-334. [3] N. Attrapadung and H. Imai, “Conjunctive broadcast and attribute-based encryption,” in Proc. Int. Conf. Pairing-Based Cryptography, 2009, pp. 248-265.

[4] B. Waters, “Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization,” in Proc. Public Key Cryptography, 2011, pp. 53-70.

[5] M. Green, S. Hohnberger, and B. Waters, “Outsourcing the decryption of ABE ciphertext,” in Proc. USENIX Secur. Symp., 2011, pp. 34.

[6] J. Lai, R. H. Deng, C. Guan, and J. Weng, “Attribute-based encryption with verifiable outsourced decryption,” IEEE Trans. Inf. Forens. Security, vol. 8, no. 8, pp. 1343-1354, 2013.

[7] S. Lin, R. Zhang, H. Ma, and M. Wang, “Revisiting attribute-based encryption with verifiable outsourced decryption,” IEEE Trans. Inf. Forens. Security, vol. 10, no. 10, pp. 2119-2130, 2015.

[8] M. Chase, and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proc. ACM CCS, 2009, 121-130.

[9] G. Zhang, L. Liu, and Y. Liu, “An attribute-based encryption scheme secure against malicious KGC,” in Proc. TRUSTCOM, 2012, pp. 1376-1380.

[10] J. Hur, “Improving security and efficiency in attribute-based data sharing,” IEEE Trans. Knowl. Data. Eng., vol. 25, no. 10, pp. 2271-2282, 2013.

[11] P. P. Chandar, D. Mutkurman, and M. Rathinrai, “Hierarchical attribute based proxy reencryption access control in cloud computing,” in Proc. ICCPCT, 2014, pp. 1565-1570.

[12] X. A. Wang, J. Ma, and F. Xhafa, “Outsourcing decryption of attribute based encryption with energy efficiency,” in Proc. 3PGCIC, 2015, pp. 444-448.

[13] L. Cheung, and C. Newport, “Provably secure ciphertext policy ABE,” in Proc. ACM CCS, 2007, pp. 456-465.

[14] J. Hur, and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214-1221, 2011.

[15] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,” in Proc. ACM CCS, 2006, pp. 99-112.

[16] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. ACM CCS, 2008, pp. 417-426.

[17] A. Xiong, C. Xu, and Q. Gan, “A CP-ABE scheme with system attributes revocation in cloud storage,” in Proc. ICCWAMIP, 2014, pp. 331-335. [18] Q. Wu, “A generic construction of ciphertext-policy attribute-based encryption supporting attribute revocation,” China Commun., vol. 11, no. 13, pp. 93-100, 2014.

[19] S. S. M. Chow, “Removing escrow from identity-based encryption,” in Proc. Int. Conf. Practice and Theory in Public Key Cryptography, 2009, pp. 256-276.

[20] M. S. Ahmad, N. E. Musa, R. Nadarajah, R. Hassan, and N. E. Othman, “Comparison between android and iOS operating system in terms of security,” in Proc. CITA, 2013, pp. 1-4.