A Collaborative Key Management Protocol in Cipher Text Policy Attribute-Based Encryption for Cloud Data Sharing

Ritesh Methalkar[1] Neha Rawandalekar[2] Priyanka Salunke[3] Sunil Mirashe[4] Prof. Mahendra Sawane[5]
[1,2,3,4,5]Genba Sopanrao Moze College of Engineering, Balewadi Pune, India

Abstract— Cipher text policy attribute-based coding (CP-ABE) may be a promising cryptologic technique for fine-grained access management of outsourced knowledge within the cloud. However, some drawbacks of key management hinder the recognition of its application. One disadvantage in pressing would like of resolution is that the key written agreement downside. we tend to indicate that front-end devices of purchasers like sensible phones typically have restricted privacy protection, therefore if personal keys square measure entirely control by them, purchasers risk key exposure that's hardly noticed however inherently existed in previous analysis. What is more, huge consumer decoding overhead limits the sensible use of ABE. During this work, we tend to propose a cooperative key management protocol in CP-ABE.

Key words: KP-ABE, CP-ABE, Cipher text, AES

I. INTRODUCTION

With cost-effectiveness improvements in computational technology and large-scale networks, sharing data with others becomes correspondingly more convenient. Additionally, digital resources are more easily obtained via cloud computing and storage. Since cloud data sharing requires off-premises infrastructure that some organizations jointly held, remote storage are somehow threatening privacy of data owners. Therefore, enforcing the protection of personal, confidential and sensitive data stored in the cloud is extremely crucial The simultaneous participation of a large number of users requires fine-grained access control for data sharing. Attribute-based encryption (ABE) is a promising cryptographic primitive that offers an interesting solution to secure and flexible data sharing. ABE has an inherent one-to-many property, which means a single key can decrypt different cipher texts or different keys can decrypt the same cipher text. There are two types of ABE, called cipher text policy ABE (CP-ABE) and key policy ABE (KP-ABE). For CP-ABE, the access policy is embedded into a cipher text and the attribute set is embedded into a private key. For KP-ABE, the access policy is embedded into a private key and the attribute set is embedded into a cipher text. CP-ABE allows data owners to define their own access policy. Anyone who wants to obtain data must first match the access policy attribute set. Due to this property, CP-ABE is quite suitable for the construction of secure, fine-grained access control for cloud data sharing.

II. LITERATURE SURVEY

Paper Name: Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems.
Author: Junbeom Hur and Dong Kun Noh.
Year: 2011

Description: In this paper, we tend to propose AN access management mechanism victimization cipher text-policy attribute- based mostly secret writing to enforce access management policies with economical attribute and user revocation capability. The fine-grained access management is achieved by twin secret writing mechanism that takes advantage of the attribute-based secret writing and selective cluster key distribution in every attribute cluster. We tend to demonstrate the way to apply the planned mechanism to firmly manage the outsourced knowledge. The analysis results indicate that the planned theme is economical and secure within the knowledge outsourcing systems. ABE comes in 2 flavours known as key-policy ABE (KP-ABE) and cipher text-policy ABE. In KP-ABE, attributes square measure wont to describe the encrypted knowledge and policies square measure designed into user's keys; whereas in CP-ABE, the attributes square measure wont to describe a user's written document, And an code or determines a policy on World Health Organization will decode the info.

Paper Name: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data
Author: Vipul Goyal, Omkant Pandeyy Amit Sahaiz Brent Waters
Year: 2011

Description: We develop a novel cryptosystem for fine-grained sharing of encrypted data that we have a tendency to tend to call Key-Policy Attribute-Based coding (KP-ABE). In our cryptosystem, ciphertexts square measure labelled with sets of attributes and private keys square measure associated with access structures that management that ciphertexts a user is prepared to decrypt. we have a tendency to tend to demonstrate the pertinence of our construction to sharing of audit-log information and broadcast coding. Our construction supports delegation of non-public keys that subsumes hierarchic Identity-Based coding (HIBE)..In our system, Fine-grained access management systems facilitate granting access rights to a group of users and allow exibility in specifying the access rights of individual users. several techniques square measure proverbial for implementing fine grained access management.

Paper Name: Ciphertext-Policy Attribute-Based Encryption: An Expressive, E_cient, and Provably Secure Realization
Author: Brent Waters
Year: 2011

Description: In our most effcient system, cipher text size, encryption, and decipherment time scales linearly with the quality of the access formula. The sole previous work to realize these parameters was restricted to a symbol within the generic cluster model. We have a tendency to gift 3 constructions at intervals our framework. Our system is tried by selection secure below a assumption that we have a tendency to decision the decisional Parallel additive Diffle - Hellman Exponent (PBDHE) assumption which may be viewed as a generalization of the BDHE assumption. Our next 2 constructions give performance tradeoffs to realize obvious security severally below the (weaker) decisional

additive- Diffle -Hellman Exponent and decisional Bilinear Di dramatist assumptions.
Paper Name: Fuzzy Identity-Based Encryption
Author: Amit Sahai, Brent Waters
Year: 2012

Description: A Fuzzy IBE theme will be applied to change cryptography victimisation biometric inputs as identities; the error-tolerance property of a Fuzzy IBE theme is exactly what permits for the utilization of biometric identities, that inherently can have some noise every time they're sampled. To boot, we have a tendency to show that Fuzzy-IBE will be used for a kind of application that we have a tendency to term "attribute-based encryption". During this paper we have a tendency to gift 2 constructions of Fuzzy IBE schemes. Our constructions will be viewed as AN Identity-Based cryptography of a message underneath many attributes that compose a (fuzzy) identity. Our IBE schemes ar each error-tolerant and secure against collusion attacks. To boot, our basic construction doesn't use random oracles. we have a tendency to prove the protection of our schemes underneath the Selective-ID security model.

III. EXISTING SYSTEM

Cipher text policy attribute-based encoding (CP-ABE) could be a promising cryptographically technique for fine-grained access management of outsourced information within the cloud. However, some drawbacks of key management hinder the recognition of its application. One downside in imperative would like of resolution is that the key written agreement drawback. we have a tendency to indicate that front-end devices of shoppers like sensible phones usually have restricted privacy protection, therefore if non-public keys square measure entirely control by them, shoppers risk key exposure that's hardly noticed however inherently existed in previous analysis. what is more, huge shopper coding overhead limits the sensible use of Attribute based mostly encoding. previous schemes of key management in attribute-based information sharing system primarily focuses on key update, proxy re-encryption and outsourced coding. Some analysis incontestable untrusted key authority could result in key written agreement drawback and provided corresponding solutions.

A. *Disadvantages of Existing System*

1) One drawback is the key escrow problem.
2) Key authority must be completely trustworthy, as it can decrypt all the cipher text using a generated private key without permission of its owner.

IV. PROPOSED SYSTEM

Propose a novel collaborative key management protocol in cipher text policy attribute-based encryption (CKM-CP-ABE) aiming to enhance security and efficiency of key management in cloud data sharing system. 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. Thus, secure key management is guaranteed without adding any extra physical infrastructure, which is easier to deploy compared with previous multi-authority schemes. 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. We indicate that not only 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 system in cloud, our proposed protocol effectively addresses both two problems by its collaborative key management. Finally, we provide proof of security for the proposed protocol. The collaborative mechanism helps markedly reduce client decryption overhead by employing a decryption server to execute most of decryption while leave no knowledge about information to it.

A. *Advantages of Proposed System*

1) In proposed system, novel collaborative protocol is presented. With help of interaction among the key authority, a cloud server and client who tends to access data, we resolve the key escrow problem.
2) Resolve Key exposure problem.

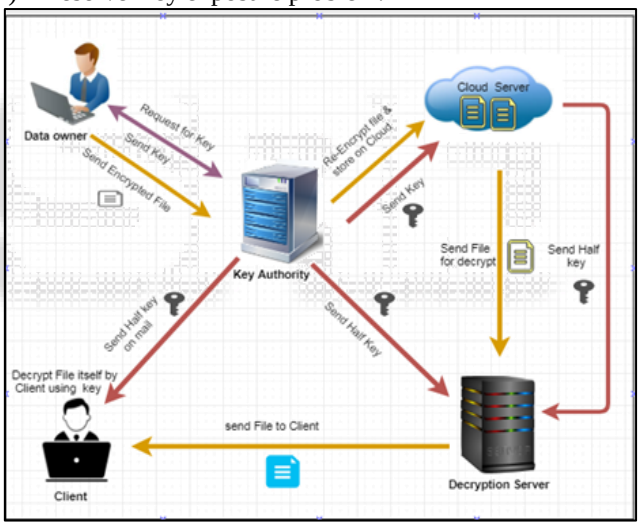

Fig. 1: System Architecture

V. ALGORITHMS

A. *Algorithm 1: AES Algorithm*

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data the data to be encrypted. This array we call the state array.

You take the following AES steps of encryption for a 128-bit block:

1) Derive the set of round keys from the cipher key.
2) Initialize the state array with the block data (plaintext).
3) Add the initial round key to the starting state array.
4) Perform nine rounds of state manipulation.
5) Perform the tenth and final round of state manipulation.
6) Copy the final state array out as the encrypted data (cipher text).

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.

These algorithm are used to file content are convert plaint text to cipher text.

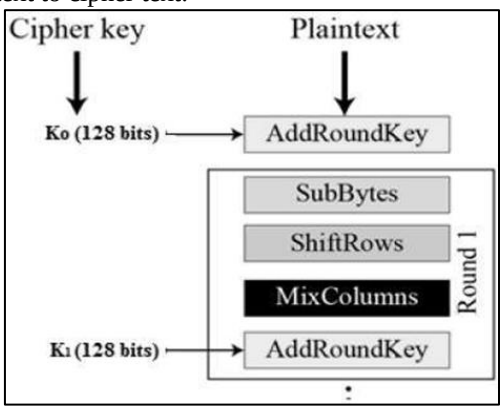

Fig. 2: AES Algorithm Diagram 1

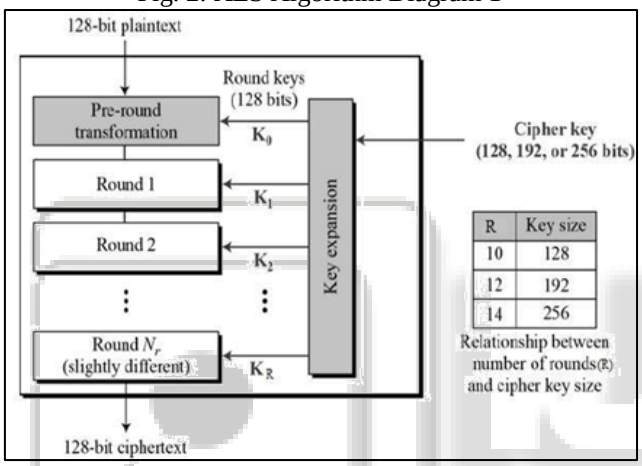

Fig. 3: AES Algorithm Diagram 2

VI. PROBLEM STATEMENT

In collaborative key management system In which existing system face key escrow problem to overcome this problem, we proposed a novel collaborative key management protocol in cipher text policy attribute-based encryption (CKM-CP-ABE) scheme enhance security and efficiency of key management in cloud data sharing system.

VII. GOALS AND OBJECTIVES

1) Attribute based data sharing.
2) Data stored in encrypted format to improve privacy.
3) Collaborative key management for resolving key escrow problem.
4) Well defined access structure for improve security.

VIII. CONCLUSION

The proposed collaborative mechanism perfectly addresses not only key escrow problem but also a worse problem called key exposure that previous research hardly noticed. Meanwhile it helps to optimize clients' user experience since only a small amount of responsibility is taken by them for decryption. Thus, the proposed scheme performs better in cloud data sharing system serving massive performance-restrained front-end devices with respect to either security or efficiency.

ACKNOWLEDGEMENTS

This work is supported by Prof. V.N Dhawas (Sinhgad Institute of Technology Lonavala)

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. EuroCrypt, 2005, pp. 457-473.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc.ACM CCS, 2006, pp. 89-98.
[3] L. Cheung, and C. Newport, "Provably secure ciphertext policy ABE," inProc. ACM CCS, 2007, pp. 456-465.
[4] 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.
[5] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive,efficient, and provably secure realization," in Proc. Public KeyCryptography, 2011, pp. 53-70.
[6] M. Green, S. Hohnberger, and B. Waters, "Outsourcing the decryption ofABE ciphertext," in Proc. USENIX Secur. Symp., 2011, pp. 34.
[7] J. Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policyattribute-based encryption," in Proc. IEEE Symp.Secur. Privacy, 2007,pp. 321-334.
[8] P. P. Chandar, D. Mutkurman, and M. Rathinrai, "Hierarchical attributebased proxy reencryption access control in cloud computing," in Proc.ICCPCT, 2014, pp. 1565-1570.
[9] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryptionwith verifiable outsourced decryption," IEEE Trans. Inf. Forens.Security, vol. 8, no. 8, pp. 1343-1354, 2013.
[10] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting attribute-basedencryption with verifiable outsourced decryption," IEEE Trans. Inf.Forens. Security, vol. 10, no. 10, pp. 2119-2130, 2015.

