ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Revocable Multi-Authority Scheme For Secure Data Access Control in Cloud Storage

Jyoti Ravasaheb Patil, Assist. Prof. P. M. Mane

Dept. of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

ABSTRACT: In cloud ensures the data security of data access control. The challenges in cloud storage system are data access control, data outsourcing and the unreliable cloud server. Ciphertext-Policy based on attributesEncryption (CP-ABE) is viewed as a standout amongst the most appropriate information get to control benefits in distributed storage, as it gives information proprietors have more straightforward control over access approaches.Furthermore, it is extremely hard to apply the ways out information straightforwardly to exist CP-ABE programs get to control for distributed storage frameworks due to issue of trait repudiation. In that, design the multi authority scheme for revocable data access control system in cloud storage system, where more authority exists contain and each authority can left attributes independently. Purpose a reparable multi-authority CP-ABE and apply it as the underlying methods to design the data access control schema.The method of withdrawing attributes you can get both forward and backward safety effectively. The results of the analysis and the simulation show that our information is proposed the access control scheme is secure in the random oracle model and is more efficient than existing.

KEYWORDS: Access control, multi-authority, CP-ABE, attribute revocation, cloud storage.

I. INTRODUCTION

CLOUDstorage is an important cloud computing service, providing services to data owners to host those data in cloud. This new paradigm of data andAccess to data services is a great challenge for data access control. Because the cloud server cannot be completely building on data owners, they can no longer rely on serversencrypt encrypted access control by attributes(CP-ABE) is considered one of the most suitabletechnologies for data access control in cloud storage systems,because it gives the data owner more direct access control [4]. In the CP-ABE scheme, there is an authority that isresponsible for attribute management and key distribution.The authority may be the registration office at a university,the human resources department in a company, etc [1]. The data owner characterizes get to approaches and encrypted information in view of strategies every client will get a mystery key mirroring its characteristics. A user can only decrypt data when their attributes meet the access policies [7].In multiple cloud storage systems, the user's attributescan be dynamically modified. A user can have the rightsome new attributes or revoked some current attributes.And your permission to access the data should be changed consequently. However, the methods of revoking existing attributesrely on a reliable or missing serverefficiency is not enough to deal with the problemattribute revocation problem in data access controlmulti-author cloud storage systems [3].In this document, we propose for the first time a revocable multi-authority authorityCP-ABE, where an efficient and secure systemthe revocation method is proposed to resolve the attributerevocation issue in the system.

II. BACKGROUND

Design the Data Access Control Scheme for more than one authoritycloud storage systems, the main challengethe problem is to build the underlying revocable multi-authority authorityCP-ABE protocol. In Chase has proposed ahowever, it cannot be the multi-authority CP-ABE protocoldirectly as the underlying techniques duetwo main reasons: 1) Security issue: Chase multiple authority [1]. The CP-ABE protocol allows the central authority to decrypt allEncrypted texts, as they contain the master key of the system;2) Release problem: Chase protocol is not supportedattribution revocation.We propose a new revocation of the new CP-ABE authorityprotocol based on the CP-EBA of a single proposed authority. That is, we extend it to the authoritarian multimake it revocable [8]. Apply the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

strategy in the Chase multi-expert CP-ABE convention to join the mystery keys produced by a few specialists for a similar client and to dodge intrigue assault.

III. MOTIVATION

1. There improve efficiency, we delegate workload Update encrypted text on the server by using proxy re-encryption. Method, so that it is also the new united user able to decipher the previously published data, which is encrypted with previous public keys, if they have sufficient attributes (security relay).
2. Improve efficiency; we move the workload of the encrypted text update from the data owners to the cloud server, so they can eliminate the huge overhead of data communication cloud owners and servers, and the high cost of calculation in data owners.

IV. LITERATURE SURVEY

1. B. Waters, ‘‘**Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization**,’’ in Proc. 4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11), 2011, pp. 53-70.
   In this paper three constructions within our framework. Our first system is selectively tested safe under the supposition that we call the parallel exponent Bilinear of e-Hellman (PBDHE), which can be considered a generalization of the BDHE assumption. Our the following two constructs provide performance commercials to achieve testable security respectively under the decisive (slope) Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman Assumptions.

2. A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ‘‘**Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption**,’’ in Proc. Advances in Cryptology-EUROCRYPT’10, 2010, pp. 62-91.
   In this document, we present two fully secure functional encryption schemes. Our first resultis a fully secure attribute encryption system (EBA). ABE previous constructionshave been shown only selectively safe. We get total security by adjusting the doubleSystem encryption methodology latest introduced by Waters and previously usedget IBE and HIBE systems fully safe. The main challenge in dual system applicationEncryption for ABE is the richest encryption of passwords and encrypted texts. In an IBE or HIBE system,Keys and encrypted texts are associated with the same kind of simple object: identity. Inan ABE system, encrypted keys, and texts are associated with more complex objects: attributesand access to formulas.

3. M. Chase and S.S.M. Chow, ‘‘**Improving Privacy and Security in Multi-Authority Attribute-Based Encryption**,’’ in Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09), 2009, pp. 121-130.
   In more authorityABE scheme, multiple attributes, authorities monitor differentset the attributes and output the corresponding decryption user and digit keys may require a userkeys for the appropriate attributes of each authority beforedecoding a message that Chase [5] has given more authorityABE that uses the concepts of a trusted central authority.(CA) and Global Identifiers (GIDs). However, CA inthat the building has the power to decipher each encrypted text,which in some way seems contradictory to the original objective ofdistributing control over many potentially unreliable authorities.

4. A.B. Lewko and B. Waters, ‘‘**Decentralizing Attribute-Based Encryption**,’’ in Proc. Advances in Cryptology-EUROCRYPT’11, 2011, pp. 568-588.
   When we build our system, our biggest technical obstacle is to make it complicated.Encryption systems based on previous attributes have given resistance to collusion when the ABE systemauthority \ bound "set of different components (representing different attributes) of a user private key that randomizes the key. However, in our system each componentcomes from a potentially different authority, where no coordination between them is assumedauthorities. We create new techniques for linking key components and avoid collusion attacks between users with different global identities.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

5. S. Yu, C. Wang, K. Ren, and W. Lou, ''**Attribute Based Data Sharing with Attribute Revocation**,'' in Proc. 5th ACM Symp.Information, Computer and Comm. Security (ASIACCS'10), 2010,pp. 261-270.
In CP-ABE, each user is associatedwith a set of attributes and data encrypted withattribute structures. A user can decrypt aEncrypted text if and only if its attributes satisfy the encryption text access structure In addition to this fundamental property, practical applications quotes generally have other requirements. In this role we focus on an important issue of withdrawing attributes thatis cumbersome for CP-ABE systems. In particular, address this challenging problem by considering it more practical scenarios where semi-trusted proxy servers areavailable.

6. M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ''**Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption**,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.
In this article we propose a new patient-centered framework and a set of mechanisms for controlling access to PHR data stored on semi-trusted servers. For accurate and scalable data access control for PHR, we use attribute-based encryption techniques (ABE) to encrypt the PHR file of each patient. Different from previous work on outsourcing secure data, we focus on the scenario of the owner of more data and we divide users into the PHR system in multiple security domains that considerably reduce the complexity of key management for owners and users. A high level of patient privacy is guaranteed simultaneously by leveraging EBAs by more authorities. Our schema also allows for dynamic modification of access policies or file attributes, supports effective revocation of user / request attributes and broken glass access in emergency scenarios.

7. J. Hur and D.K. Noh, ''**Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems**,'' IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
In this role, it proposes an access control mechanism that uses cryptographic text attribute-based encryption to enforce access control policies the efficient attribute and the ability to revoke the user. The metric access control can be achieved through a dual coding mechanism that uses attribute-based cryptography and selective distribution of the group key in each attribute group. Let's show how implement the proposed mechanism to manage outsourced data safely.

8. S. Jahid, P. Mittal, and N. Borisov, ''**Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation**,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.
We achieve this by creating a proxy that participates in the process of decryption and imposes the revocation limitations The proxy is a minimum trust and cannotdecrypt encrypted texts or provide access to previously revoked onesusers. We describe the architecture and construction of EASIER, provide performance evaluation and application of prototypes of our focus on Facebook.

9. K. Yang and X. Jia, ''**Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage**,'' in Proc. 32th IEEE Int'l Conf. Distributed Computing Systems (ICDCS'12), 2012, pp. 1-10.
In this document we have designed an access control framework for more authority systems and propose an efficient and secure solutionmulti-authority access control system for cloud storage. We firstDesign an efficient multi-authority CP-ABE system that it does not require a global authority and can support any LSSS access structure. So, try your security in the random oracle model.We also propose a new technique to resolve attribution revocationproblem in multi-authoritative CP-ABE systems.

V. EXISTING SYSTEM

This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can longer rely on server to do access control. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is viewed as a standout amongst the most appropriate innovations for

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

information get to controls in proprietor more straightforward control on get to approaches. In CP-ABE plot, there is an expert that is in charge of quality administration and key appropriation.

Disadvantages of Existing System

1. Chase's multi-authority CP-ABE protocol allows the central authority to decrypt all the ciphertexts, since it holds the master key of the system.
2. Chase's protocol does not support attribute revocation.

VI. PROPOSED SYSTEM

In that, firstly propose a revocable multi authority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system. Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, both backward security forward securities. Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi-trusted in some.

Advantages of Proposed System:

1. We modify the framework of the scheme and make it more practical to cloud storage systems, in which data owners are not involved in the key generation.
2. We greatly improve the efficiency of the attribute revocation method.
3. We also highly improve the expressiveness of our access control scheme, where we remove the limitation that each attribute can only appear at most once in a ciphertext.

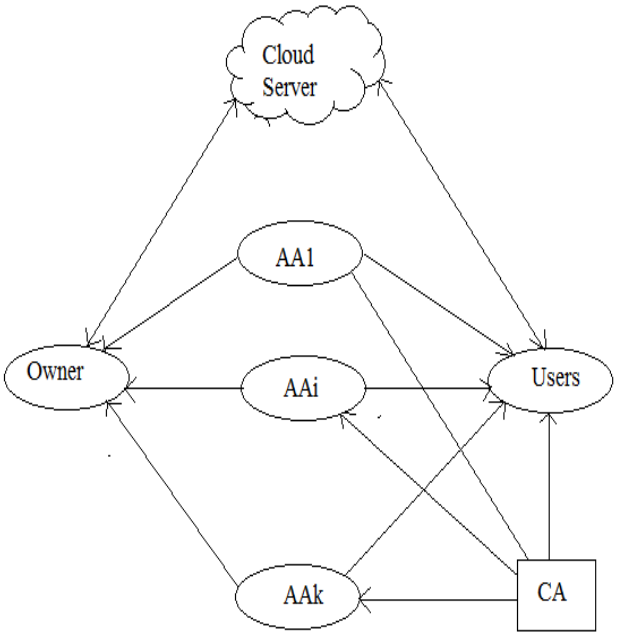

Fig. System Architecture

VII. CONCLUSION

In that, proposea revocable multi-authority CPABE plot that can bolster successful attribution disavowal.Then, develop an effective data access controlfor cloud storage systems with multiple authors. Who we arehas also shown that our scheme has been proven safe in therandom oracle model. The CPABE can be denied multi-specialist is a promising

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

method, which can be connected to any one remote stockpiling frameworks and online informal organizations, and so on.

REFERENCES

[1] B. Waters, ''Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,'' in Proc. 4th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC'11), 2011, pp. 53-70.
[2] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ''Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'10, 2010, pp. 62-91.
[3] M. Chase and S.S.M. Chow, ''Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,'' in Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), 2009, pp. 121-130.
[4] A.B. Lewko and B. Waters, ''Decentralizing Attribute-Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11, 2011, pp. 568-588.
[5] S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS'10), 2010, pp. 261-270.
[6] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.
[7] J. Hur and D.K. Noh, ''Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,'' IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
[8] S. Jahid, P. Mittal, and N. Borisov, ''Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.
[9] K. Yang and X. Jia, ''Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,'' in Proc. 32th IEEE Int'l Conf. Distributed Computing Systems (ICDCS'12), 2012, pp. 1-10.