Revocable Multi-Authority CP-ABE Scheme

[1]G.Sagana, [2]R.Deepalakshmi, [3]Mrs.P.Vijayalakshmi,

[1,2]PG Scholar , [3]Assistant Professor
Department of MCA, Panimalar Engineering College

Abstract

Data read control is an effective way to ensure the data self-assurance in the cloud. Due to data farm out and untrusted cloud servers, the data read control becomes a challenging broadcast in cloud loading systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data read control in cloud loading, because it gives data owners more direct control on read rules. However, it is hard to directly apply existing CP-ABE system to data access control for cloud loading systems because of the elements overturning problem., we design anexpressive,efficient and revocable data access control system for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to broadcast elements independently. Specifically, we suggest a revocable multi-authority CP-ABE system, and apply it as the underlying techniques to design the data access control scheme. Our elements overturning method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our suggest data access control scheme is secure in the random oracle model and is more efficient than previous works.

Keywords—*The read control, multi-authority, CP-ABE (ciphertext policy attribute encryption scheme), elements overturning, cloud loading.*

I. INTRODUCTION

CLOUD loading is an important service of cloud estimating, which compromises services for data owners to host their data in the cloud. This new hypothesis of data hosting and data access services introduces a great task to data read control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do read control. Ciphertext-Policy Attribute-based Encryption(CP-ABE) is considered as one of the most appropriate technologies for data read control in cloud loading systems, because it gives the data owner more obvious control on read rules.

The CP-ABE scheme, there is an evidence that is conscientious for elements management and key allocation .The evidence can be the check office in a academia, the human resource department in a company, etc. The data owner defines the read rules and encrypts data according to the rules. Each user will be delivered a confidence key redirecting its elements. A user can decrypt the data only when its elements satisfy the read rules.

There are two types of CP-ABE systems: single-authority CP-ABE where all elementes are managed by a single- authority, and multi-authority CP-ABE where elements are from different domains and managed by different evidences. Multi-authority CP-ABE is more appropriate for data read control of cloud loading systems, as users may hold read delivered by multiple evidences and data owners may also share the data using read rules defined over read from different evidences.

II. PURPOSE OF THE PROJECT

Before file allocation the user pre-computes a certain number of short substantiation demonstrations on separate vector. User wants to make sure the loading appropriateness for the data in the cloud, the tasks the cloud servers with a set of unintentionally generated block indices. Each cloud server computes a short "signature" over the detailed blocks and returns them to the user.

Error localization is a key prerequisite for eliminating errors in loading systems. Our system outperforms those by participating the accuracy.

Authentication and error localization (misbehaving server identification) in our challenge-response procedure: The response values from servers for each task not only determine the acceptability of the allocated loading, but also contain data to locate potential data error(s).

The user can rebuild the original file by downloading the data vectors from the first m servers, assuming that they return the accurate reaction values. That our substantiation system is based on accidental spot-checking, so the loading exactness self-confidence is a probabilistic one. The data exploitation is detected, the comparison of pre-computed demonstration and received response values can assurance the identification of misbehaving server(s) (again with high probability), which will be discussed shortly.

III. SYSTEM STUDY

A. Existing System

This new hypothesis of data hosting and data read facilities announces a unlimited task to data read control. Because the cloud server cannot be fully trusted by data owners, they can no extensive rely on servers to do read control.

Ciphertext-Policy Attribute-based Encryption (CP-ABE) is observed as one of the most appropriate machineries for data read control in cloud loading systems, because it gives the data owner more unequivocal control on read rules.

CP-ABE scheme, there is an conviction that is responsible for elements management and key allocation.

B. Disadvantages

The pursuit's multi-authority CP-ABE procedure allows the crucial evidence to decrypt all the ciphertexts, since it storages the controller key of the system.

The pursuits procedure does not support elements annulment.

C. Proposed System

The first suggest a revocable multiauthority CP-ABE scheme, where an capable and assured annulment method is suggested to solve the elements annulment problem in the system.

Our elements annulment method is capable in the sense that it acquires less consultation cost and estimation cost, and is self-confident in the sense that it can accomplish both backward security (The rescinded user cannot decrypt any new ciphertext that obliges therescinded elements to decrypt) and forward security (The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient,elements).

Our system does not oblige the server to be fully confidential, because the key update is coerced by each elements evidence not the server. Even if the server is not semi confidential in some consequences, our system can still assure the backward security.

Then, we apply our suggested revocable multi-authority CP-ABE scheme as the underlying methods to build the sensitive and self-assured data read control system for multi-authority cloud loading systems.

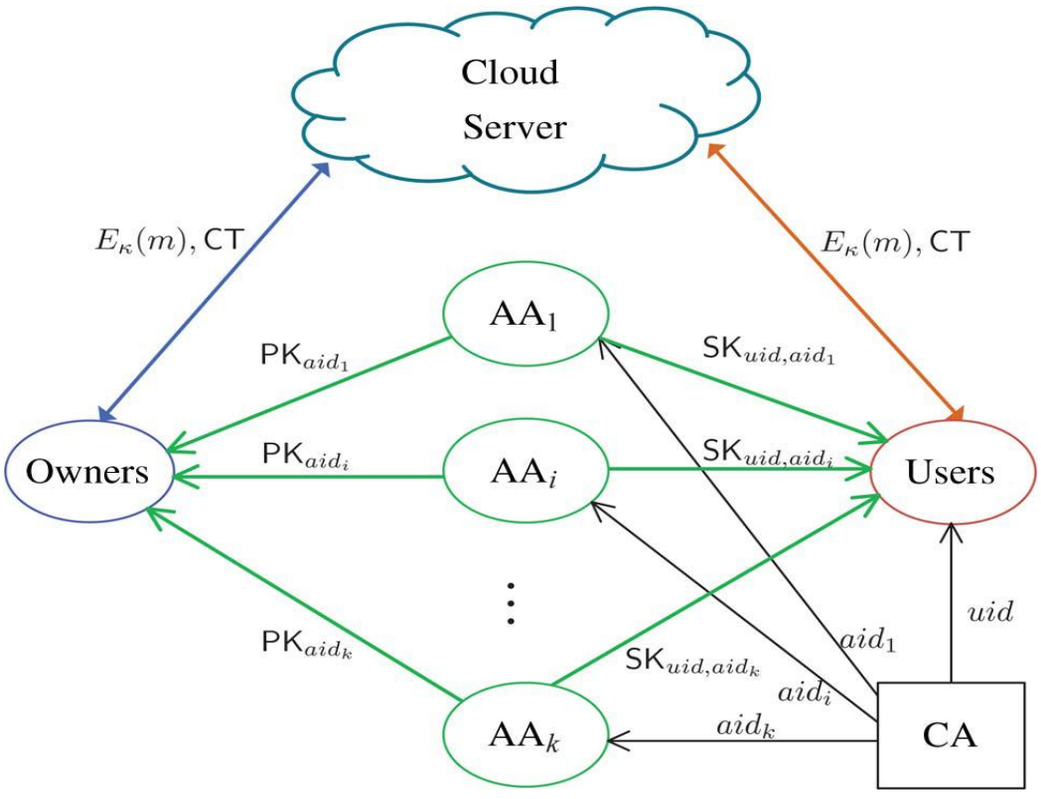
D. Advantage

To transform the construction of the system and make it more concrete to cloud loading systems, in which data owners are not involved in the key origination.

The critically improve the effectiveness of the elements annulment method.

It also highly improve the articulacy of our read control system, where we eliminate the restriction that each elements can only appear at most once in a ciphertext.

IV. ARCHITECTURE



V. IMPLEMENTATION

A. System model:

A demonstrative network construction for cloud loading service demonstrative iselucidated in this module. Three different network creatures can be identified as follows:

B. User:

An creature, who has data to be loading in the cloud and distrusts on the cloud for data loading and estimation, can be either creativity or discrete customers.

C. Cloud Server(CS)

An crearure, which is achieved by cloud service provider (CSP) to provide data loading service and has substantial loading space and estimation capitals (we will not differentiate CS and CSP hereafter.).

D. Certificate Authority (CA)

An optional CA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

THERE ARE THREE ALGORITHMS TO BE USED, SUCH THAT,

- Token pre-computation
- Correctness verification and Error localization
- Error recovery.

1) Token Pre-Computation

Before file allocation the user pre-computes a certain number of abruptly substantiation reminders on distinctive vector.

User wants to make sure the loading accuracy for the data in the cloud, he encounters the cloud servers with a set of accidentally generated block indices.

Each cloud server computes a short "signature" over the specified blocks and returns them to the user.

2) Correctness Verification And Error Localization

Error localization is a key qualification for excluding errors in loading systems.

Our system outstrips those by assimilating the accuracy substantiation and error localization (misbehaving server identification) in our challenge-response protocol.

3) Error recovery:

The user can rebuild the original file by transforming the data vectors from the first m servers, assuming that they return the appropriate reaction values.

That our substantiation system is based on accidental spot-checking, so the loading accuracy self-confidence is a probabilistic one.

The data degeneracy is detected, the association of pre-computed demonstrations and received response values can assurance the identification of misbehaving server(s) (again with high probability), which will be discussed shortly.

VI. CONCLUSION AND FUTURE WORK

we suggested a revocable multi-authority CPABE scheme that can support efficient elements annulment .Then, we created an effective data read control system for multi-authority cloud loading systems. We also proved that our system was provable self-confident in the deliberate prediction model. The revocable multi-authority CPABE is a promising technique, which can be applied in any remote loading systems and online social networks etc.

REFERENCES

[1] P. Mell and T. Grance, ''The NIST Definition of CloudComputing,'' National Institute of Standards and Technology,Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-Policy Attribute-Based Encryption,'' in Proc. IEEE Symp. Security and privacy (S&P'07), 2007, pp. 321-334.

[3] 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.

[4] V. Goyal, A. Jain,O. Pandey, andA. Sahai, ''Bounded Ciphertext Policy Attribute Based Encryption,'' in Proc. 35th Int'l Colloquium on Automata, Languages, and Programming (ICALP'08), 2008,pp. 579-591.

[5] 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.

[6] M. Chase, ''Multi-Authority Attribute Based Encryption,'' in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography(TCC'07), 2007, pp. 515-534.

[7] 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.

[8] A.B. Lewko and B. Waters, ''Decentralizing Attribute-Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11,2011, pp. 568-588.

[9] 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.

[10] 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.