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. 6, Issue 11, November 2018

A New Threshold Multi-Authority CP-ABE Access Control Scheme in Public Cloud Storage

Changala Priyanka[1], J.Raghunath[2]

M.Tech Student, Dept. of CSE, Gates Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India [1]

Assistant Professor, Dept. of CSE, Gates Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India[2]

ABSTRACT: Data access control is an efficient way to provide the data security in the cloud but due to data outsourcing over untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Attribute-based Encryption (ABE) technique is regarded as a most trustworthy cryptographic conducting tool to guarantee data owner's direct control on their data in public cloud storage. The previous ABE schemes involve only one authority to maintain the complete attribute set, which can bring a single-point hindrance on both security and performance. In this paper, from another perspective, we conduct a threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, in which multiple authorities jointly manage a uniform attribute set and every authority is able to issue attributes independently..

KEYWORDS: Querying, multi-dimensional data, indexing, hashing

I.INTRODUCTION

Cloud computing is meant to satisfy requirement of data storage and data outsourcing for data owners. Thought cloud service provides such services but security and privacy of owner's data is major concern in cloud storage. Therefore secure data access is critical issue in cloud storage. Attribute-Based Encryption (ABE) is one of the suitable techniques to access data securely on cloud where control of data access is in the hand of data owner. Ciphertext- Policy Attribute-Based Encryption (CP-ABE) is among the category of ABE scheme where, data owners can define access policy for each file based on users attribute. In most existing CP-ABE scheme the attribute managed and key distribute only by one authority. Thus one authority can lead system toward single point failure which directly effect on system performance and security. In this case single point failures can occur. In multi-authority CP-ABE scheme, the whole attribute set is divided into multiple subsets, each subset is now maintained by single authority. In this case adversary cannot compromise all authority at a same time. In addition single point failure has not solved. Another technique which solves the problem of single point failure is Threshold multi-authority CP-ABE access control that is TMACS. In this technique multiple authorities jointly manage the whole attribute set but no one has full control over any specific attribute. In this technique secret sharing key is used among different authorities with (t, n) threshold secret sharing. In TMACS secrete key is known as a Master Key which cannot be obtained by any single authority alone.

II. LITERATURE SURVEY

Distributed, Concurrent and Independent Access to Encrypted Cloud Databases is the encrypted cloud database access provides multiple, independent and geographically distributed client to execute concurrent queries on encrypted data. Here even SQL statements are in modified encrypted structure to provide confidentiality. The above goals are designed by proxy less cloud-client communication. To achieve goals like availability, scalability, SecureDBaaS prototype is used to support mentioned goals. Here SecureDBaaS process plaintext data, encrypted data, metadata and encrypted metadata. Data and metadata are stored in cloud database. SecureDBaaS clients can retrieve the required metadata from cloud through SQL statements. Secure table contain data where secure table is nothing but encrypted tables. The problem with this approach is all the SQL commands types need to predefine during design phase which seems impractical i.e. the set of SQL operations does not change after database design. In Adaptive encryption

DOI: 10.15680/IJIRCCE.2018. 0611019

architecture for cloud databases this approach access to cloud is adaptive that is change in workload doesn't cost to performance degradation, it also bring us privileges to change the set of SQL queries even after database design. This is proxy less architecture.

All metadata and data are stored in cloud database and can access by client through encrypted database engine. Encrypted engine fetch required metadata to execute SQL queries from cloud database and decrypt it through master key which is with client side application. Adaptive encryption scheme consider many SQL aware encryption algorithm such as Random, Deterministic which supports equality operators, order preserving encryption, homomorphic sums, plain and search. Adaptive encryption scheme consider many SQL aware encryption algorithm such as Random, Deterministic which supports equality operators, order preserving encryption, homomorphic sums, plain and search. If each column is encrypted through only one algorithm then administrator has to decide database operations at design time only for each column. Here encryption algorithms are organized into structure called onions, where each onion is made up of ordered set of encryption algorithm called layer. Onions layers are used for equality, comparison, summation, string equality operators. Each plaintext column is encrypted into one or more encrypted column each one corresponding to an onion. Each plain text is encrypted through all the layers of its onion i.e., encrypted through more than on encryption algorithm. Thought this approach provides more adaptive mechanism for accessing cloud database, access policies are assigned by data owner or single authority only which can result in system bottleneck.

Multi-User Encrypted SQL Operation on Cloud approach provides scalable and confidential access to cloud database. This architecture called Multi-User relational Encrypted Data Base (Mute DB) that guarantees data confidentiality by executing SQL operation on data by applying access control policies. The Mute DB does not rely on any intermediate proxy to avoid single point bottleneck. Here every data and metadata is stored on cloud in encrypted format. Here data managed and create by DBA, who is also responsible storing encrypted data and metadata on the cloud. DBA is the trusted entity who owns root credentials, manages user accounts and enforces access control policies. This ACP defines which user can have access on which data. Each user will be provided set of credentials including all the information that allows him/her to access legitimate data. In this case access policies are also encrypted and stored in cloud. The DBA is the only authority who can have control on all system entity; this can leads toward DBA overloading and can result on performance degradation.

III. EXISTING SYSTEM

Attribute-based Encryption (ABE) is regarded as one of the most suitable schemes to conduct data access control in public clouds for it can guarantee data owners' direct control over their data and provide a fine-grained access control service. Till now, there are many ABE schemes proposed, which can be divided into two categories: Key-Policy Attribute-based Encryption (KP-ABE) and Ciphertext-Policy Attribute-based Encryption (CP-ABE).

In KP-ABE schemes, decrypt keys are associated with access structures while ciphertexts are only labeled with special attribute sets. On the contrary, in CP-ABE schemes, data owners can define an access policy for each file based on users' attributes, which can guarantee owners' more direct control over their data. Therefore, compared with KP-ABE, CP-ABE is a preferred choice for designing access control for public cloud storage.

IV.PROPOSED WORK

In this paper, we propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes.
In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t; n) threshold secret sharing into our scheme to share the secret key among authorities.

In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t; n) threshold secret sharing guarantees that the master key cannot be obtained by any authority alone.

ARCHITECTURE

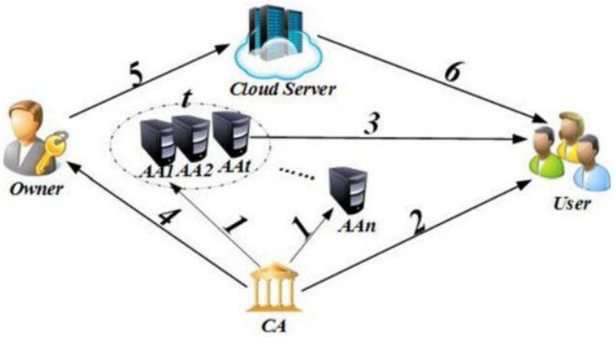

Fig 1 System Architecture.

IMPLEMENTATION

TMACS

The TMACS multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. In TMACS, a global certificate authority is responsible for the construction of the system, which avoids the extra overhead caused by AAs' negotiation of system parameters. CA is also responsible for the registration of users, which avoids AAs synchronized maintaining a list of users. However, CA is not involved in AAs' master key sharing and users' secret key generation, which avoids CA becoming the security vulnerability and performance bottleneck. Design of TMACS is reusing of the master key shared among multiple attribute authorities. In traditional (t;n) threshold secret sharing, once the secret is reconstructed among multiple participants, someone can actually gain its value. Similarly, in CP-ABE schemes, the only-one-authority knows the master key and uses it to generate each user's secret key according to a specific attribute set. In this case, if the AA is compromised by an adversary, it will become the security vulnerability. To avoid this, by means of (t;n) threshold secret sharing, the master key cannot be individually reconstructed and gained by any entity in TMACS.hat the master key a is actually secure. By this means, we solve the problem of reusing of the master key.

Data Access Control Scheme:

We propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes. In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t;n) threshold secret sharing into our scheme to share the secret key among authorities. In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t;n) threshold secret sharing guarantees that the master key cannot be obtained by any authority alone. TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. To the best of our knowledge, this paper is the first try to address the single point bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

Certificate authority:

The certificate authority is a global trusted entity in the system that is responsible for the construction of the system by setting up system parameters and attribute public key (PK) of each attribute in the whole attribute set. CA accepts users and AAs' registration requests by assigning a unique uid for each legal user and a unique aid for each AA. CA also decides the parameter t about the threshold of AAs that are involved in users' secret key generation for each time. However, CA is not involved in AAs' master key sharing and users' secret key generation. Therefore, for example, CA can be government organizations or enterprise departments which are responsible for the registration. Certificate authority is responsible for the construction of the system, which avoids the extra overhead caused by AAs' negotiation of system parameters. CA is also responsible for the registration of users, which avoids AAs synchronized maintaining a list of users.

Attribute authorities:

The attribute authorities focus on the task of attribute management and key generation. Besides, AAs take part of the responsibility to construct the system, and they can be the administrators or the managers of the application system. Different from other existing multi-authority CP-ABE systems, all AAs jointly manage the whole attribute set; however, any one of AAs cannot assign users' secret keys alone for the master key is shared by all AAs. All AAs cooperate with each other to share the master key. By this means, each AA can gain a piece of master key share as its private key, then each AA sends its corresponding public key to CA to generate one of the system public keys. When it comes to generate users' secret key, each AA only should generate its corresponding secret key independently. The master key shared among multiple attribute authorities. In traditional (t;n) threshold secret sharing, once the secret is reconstructed among multiple participants, someone can actually gain its value.

V. CONCLUSION

A robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS is proposed, to deal with the single-point bottleneck on both security and performance in most existing schemes. In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t; n) threshold secret sharing into our scheme to share the secret key among authorities. In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t; n) threshold secret sharing guarantees that, the master key cannot be obtained by any authority alone. TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. To the best of our knowledge, this paper is the first try to address the single point bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Instit. Standards Technol., vol. 53, no. 6, p. 50, 2009.
[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. 14th Financial Cryptography Data Security, 2010, pp. 136–149.
[3] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan.-Feb. 2012.
[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 457–473.
[5] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. 14th ACM Conf. Comput. Commun. Security, 2014, pp. 195–203.
[6] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proc. 29th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2010, pp. 62–91.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
[8] N. Attrapadung, B. Libert, and E. Panafieu, "Expressive keypolicy attribute-based encryption with constant-size ciphertexts," in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography, 2011, pp. 90–108.
[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute- based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.
[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography, 2011, pp. 53–70.
[11] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proc. 35th Int. Colloquium Automata, Lang. Programm., 2008, pp. 579–591.
[12] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. 14th Eur. Symp. Res. Comput. Security, 2009, pp. 587–604.

[13] M. Chase, "Multi-authority attribute based encryption," in Proc. 4th Theory Cryptography Conf., 2007, pp. 515–534.

BIOGRAPHY

Mrs. CHANGALA PRIYANKA RECEIVED B.TECH DEGREE IN INFORMATION TECHNOLOGY FROM JNTUA,ANANTAPUR UNIVERSITY AND STUDYING MASTERS DEGREE IN COMPUTER SCIENCE & ENGINEERING IN GATES INSTITUTE OF TECHNOLOGY,GOOTY,AFFILIATED TO JNTUA ,ANANTAPUR ,A.P.

Mr.J.RAGHUNATH IS CURRENTLY WORKING AS AN ASSISTANT PROFESSOR IN CSE DEPARTMENT.GATES INSTITUTE OF TECHNOLOGY.HE RECEIVED B.TECH DEGREE FROM GATES INSTITUTE OF TECHNOLOGY,JNTUH,A.P&M.TECH DEGREE FROM JNTUA UNIVERSITY,JNTUA,A.P.HE HAS PUBLISHED RESEARCH PAPERS IN VARIOUS NATIONAL &INTERNATIONAL JOURNALS & CONFERENCE ACROSS THE GLOBE