INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 3, Issue 6)
Available online at www.ijariit.com

A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage

Manisha More
Computer Science & Engineering,
Matoshri Prathishthan Group of Institutions,
Nanded, India
mani.tobre@gmail.com

Shital Y. Gaikwad
Computer Science & Engineering
Matoshri Prathishthan Group of Institutions,
Nanded, India
shitalygaikwad@gmail.com

Abstract: Attribute-based Encryption is observed as a promising cryptographic leading tool to assurance data owners' direct regulator over their data in public cloud storage. The former ABE schemes include only one authority to maintain the whole attribute set, which can carry a single-point bottleneck on both security and performance. Then, certain multi-authority schemes are planned, in which numerous authorities distinctly maintain split attribute subsets. However, the single-point bottleneck problem remains unsolved. In this survey 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. In TMACS, taking advantage of (t, n) threshold secret allocation, the master key can be shared among multiple authorities, and a lawful user can generate his/her secret key by interacting with any t authorities. Security and performance analysis results show that 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. Also, by efficiently combining the traditional multi-authority scheme with TMACS, we construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

Keywords: Cloud, DBA, Public Key, TMACS, Multi-authority.

I. INTRODUCTION

Now a day's cloud computing is an intelligently developed technology to store data from a number of the client. Cloud computing allows users to remotely store their data over cloud. The remote backup system is the progressive technique which minimizes the cost of implementing more memory in an organization. It helps government agencies and enterprises to reduce the financial overhead of data management. They can extract their data backups remotely to third party cloud storage providers than maintaining their own data centres. An individual or an organization does not require purchasing the storage devices. Instead, they can store their data in the cloud and archive data to avoid information loss in case of system failures like hardware or software failures. Cloud storage is extra supple, but security and privacy are accessible for the outsourced data become a thoughtful anxiety. To attain secure data transaction in the cloud, suitable cryptography method is used. The data owner must after encryption of the file, store to the cloud. If a third person downloads the file, they can view the record if they had the key which is used to decrypt the encrypted file. To overcome the problem Cloud computing is one of the emerging technologies, which contains huge open distributed system. It is important to protect the data and privacy of user [1].

A public cloud is one in view of the standard distributed computing model, in which an administration supplier makes assets, for example, applications and capacity, accessible to the overall population over the Internet. The fundamental advantages of utilizing an open cloud administration are simple and reasonable set-up in light of the fact that equipment, application, and transmission capacity expenses are secured by the supplier, Versatility to address issues. To fulfil necessities of information stockpiling and elite calculation, distributed computing has drawn broad considerations from both scholastic and industry. Cloud capacity is an essential administration of distributed computing, which gives administrations to information proprietors to outsource information to store in the cloud through the Internet.

Regardless of numerous points of interest of distributed storage, there still stay different testing obstructions, among which, protection, what's more, security of clients' information have gotten to be significant issues, particularly in broad daylight distributed storage. Customarily, an information proprietor stores his/her information in trusted servers, which are for the most part controlled by a completely trusted chairman. In any case, in broad daylight distributed storage frameworks, the cloud is typically kept up and oversaw by a semi-trusted third party (the cloud supplier). Information is no more in information proprietor's trusted areas and the information proprietor can't trust on the cloud server to direct secure information get to control. Consequently, the safe get to control issue has turned into a basic testing issue openly distributed storage, in which customary security advancements can't be straightforwardly connected.

II. LITERATURE SURVEY

Distributed, Concurrent and Independent Access to Encrypted Cloud Databases is the encrypted cloud database access provides a 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 a cloud database. SecureDBaaS clients can retrieve the required metadata from cloud through SQL statements. Secure table contains data where the 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 architecture for cloud databases this approach access to cloud is adaptive that is a 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 [4].

III. RELATED WORK

Cryptographic techniques are well applied to access control for cloud storage system.[3]The data owners encrypt files by using the symmetric encryption approach with content keys and then use every user’s public key to encrypt the content keys. Attribute-based Encryption (ABE) is a promising technique that is very suitable for access control of encrypted data. In CP-ABE schemes,[2] 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 existing access control systems for public cloud storage, there brings a single-point bottleneck on both security and performance against the single authority for any specific attribute [2]. By introducing the combining of (t;n) threshold secret sharing and multi-authority CP-ABE scheme we propose multi- authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set. By combining the traditional multi authority scheme with ours, we construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities which can solve single point bottleneck problem and provide security.

IV. EXISTING SYSTEM AND ITS MODULES DESCRIPTION

There is only one authority responsible for attribute management and key distribution. This only-one-authority scenario can bring a single-point bottleneck on both security and performance. Once the authority is compromised, an adversary can easily obtain the only-one-authority’s master key, and then he/she can generate private keys of any attribute sub set to decrypt the specific encrypted data. Crash or offline of a specific authority will make that private keys of all attributes in attribute subset maintained by this authority cannot be generated and distributed, which will still influence the whole system’s effective operation.

1. This only-one-authority scenario can bring a single point bottleneck on both security and performance.
2. These CP-ABE schemes are still far from being widely used for access control in public cloud storage.

Module Description:

A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage have three modules

1. User module
2. Multi authority Access control
3. Public cloud storage

User Module: In this module, Users are having authentication and security to access the detail which is presented in the system. Before accessing or searching the details user should have the account in that otherwise they should register first.

Multi-authority Access Control: 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. To the best of our knowledge, we are the first to design multi authority access control architecture to deal with the problem. To satisfy this hybrid scenario, we conduct a hybrid multi-authority access control scheme, by combining the traditional multi-authority scheme with our proposed TMACS.

Public Cloud Storage: Cloud storage is an important service of cloud computing which provides services for data owners to outsource data to store in cloud via Internet. The cloud server is always online and managed by the cloud provider. Usually, the cloud server and its provider is assumed “honest-but-curious”. The cloud server does nothing but provide a platform for owners storing and sharing their encrypted data. The cloud server doesn’t conduct data access control for owners [4].

V. PROPOSED MODULE

1. Certificate Authority: Certificate Authority is responsible for the construction of the system by setting up system parameters and attribute public key(PK) of each attribute in whole attribute set.

2. Attribute authority: Attribute authority focuses on the attribute management and key generation. AA jointly manages the whole attribute set , any one of the AA cannot assign users secrete key alone for the master key is shared by AA.

3. Data Owner: Owner encrypts his/her file and define access about who can get access to his/her data. Owner encrypts his/her data with a symmetric encryption algorithm .Then the owner formulates access policy over an attribute set and encrypts the symmetric key under the policy according to attribute public key gained from CA .

4. Data Consumer: In this module, Users are having authentication and security to access the detail which is presented in the system. Before accessing the details user should have the account in that otherwise they should register first. CA can assign user identity uid and password to data consumer. [2]

5. Public Cloud Server: An entity which is managed by cloud server provider to provide data storage services. In cloud data storage , a user store his data in cloud server .In cloud data storage system , user store their data in clouds and no longer possess the data locally. Thus the correctness and availability of the data files being stored on the distributed cloud server must be guaranteed.

VI. APPLICATION

1. In medical field for insurance claim activity.
2. We design an access control framework for multi-authority systems and propose an efficient and secure multi-authority access control scheme for cloud storage.
3. We first design an efficient multi-authority CP-ABE scheme that does not require a global authority.

VII. CONCLUSION

In this paper, we proposed multi-authority access control scheme, in public cloud storage. In this scheme multiple authority jointly manages the whole attribute set and share the master key. This scheme avoids a single-point bottle neck on both security and performance.

REFERENCES

1. Multi-Authority Data Access Control For Cloud Storage System With Attribute-Based Encryption, G. V. Kapse, Dr. V. M. Thakare, Prof. S. S. Sherekar, A. V. Kapse, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727, PP 53-59.
2. Wei Li, KaipingXue, YingjieXue, and Jianan Hong. “TMACS: A Robust and Verifiable Threshold Multi Authority Access Control System in Public Cloud Storage” VOL. 27, NO. 5, MAY 2016.
3. K. Yang and X. Jia, “Attributed-based access control for multi-authority systems in cloud storage,” in Proc. IEEE 32nd Int. Conf.Distrib. Comput. Syst., 2012, pp. 536–545.
4. A Provable Threshold Multi-Authority Access Control System in Public Cloud Storage, K. K. NIKHIL, International Journal of Advanced Technology and Innovative Research Volume. 08, IssueNo.21, November-2016, Pages: 4037-4041.

5. Shivprasad Nardele, Amol Vilegave, Abhijeet Thete, Darshak Trivedi, A Robust and Verifiable Threshold Multi Authority Access Control System in Public Cloud Storage, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 11, November 2016, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798.
6. A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
7. T. Pedersen, “A threshold cryptosystem without a trusted party,” in Proc. 10th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 1991, pp. 522–526.
8. T. Jung, X. Li, Z. Wan, and M. Wan, “Privacy preserving cloud data access with multi-authorities,” in Proc. 32nd IEEE Int. Conf. Comput. Commun. 2013, pp. 2625–2633.