|| Volume 3 || Issue 5 || May 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Efficient Auditable Access Control Systems for Public Shared Cloud Storage

Vidya Patil[1], Prof. Varsha R. Dange[2]
Student, Department of Computer Science Dhole Patil College of Engineering, Pune, Maharashtra, India[1]
Assistant Professor, Department of Computer Science Dhole Patil College of Engineering, Pune, Maharashtra, India[2]

ABSTRACT: In public cloud storage system protecting the data and controlling the data access is a challenging issue. Cipher text Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However numerous works have been proposed using CP-ABE scheme, in which the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. Clients may be stuck in the waiting line for a long stretch to get their mystery keys, which results in low-efficiency of the framework. Even though the multi authority access control plans have been proposed, these plans still cannot conquer the disadvantages of single-point bottleneck and low efficiency; because of the way that each of the authority still autonomously deals with a disjoint characteristic set. In this work, it has been proposed a novel heterogeneous framework to remove the problem of single point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism. This framework employs multiple attribute authorities to share the load of user legitimacy verification. Meanwhile, in this scheme, a CA (Central Authority) is introduced to generate secret keys for legitimacy verified users and each of the authorities in our scheme manages the whole attribute set individually. This system makes performance improvement in key generation and also guarantees security requirement.

KEYWORDS: *Cloud storage, Access control, Auditing, CPABE.*

I INTRODUCTION

Cloud computing has drawn extensive attentions from both academic and industry to satisfy the requirement of data storage and high performance computations. Cloud storage is an important service of cloud computing which provides services for data owners to outsource data to store in cloud via Internet. Benefits of using cloud storage include greater accessibility, higher reliability, rapid deployment and stronger protection, to name just a few. Despite the mentioned benefits, this paradigm also brings forth new challenges on data access control, which is a critical issue to ensure data security. Since cloud storage is operated by cloud service providers, who are usually outside the trusted domain of data owners, the traditional access control methods in the Client/Server model are not suitable in cloud storage environment. The data access control in cloud storage environment has thus become a challenging issue. To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Cipher text Policy Attribute- Based Encryption (CP-ABE) is regarded as one of the most promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine grained and secure access control for cloud storage systems. In CP-ABE schemes, the access control is achieved by using cryptography, here an owners data is encrypted with an access structure over attributes, and a users secret key is labeled with his/her own attributes. Only if the attributes associated with the users secret key satisfy the access structure, can the user decrypt the corresponding cipher-text to obtain the plaintext. So far, the CP-ABE based access control schemes for cloud storage have been developed into two complementary categories, namely, single-authority scenario and multi authority scenario. In most existing CP-ABE schemes 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-authorities master key, and then he/she can generate private keys of any attribute subset to decrypt the specific encrypted data. Moreover, once the only-one-authority is crashed, the system completely cannot work well. Therefore, these CP-ABE schemes are still far from being widely used for access control in public cloud storage. Although some multi-authority CP-ABE schemes have been proposed, they still cannot deal with the problem of single-point bottleneck on both security and performance mentioned above. In these multi-authority CP-ABE schemes, the whole attribute set is divided into multiple disjoint subsets and each attribute subset is still maintained by only one authority. A straightforward idea to remove the single-point bottleneck is to allow multiple authorities to jointly manage the universal attribute set, in such

a way that each of them is able to distribute secret keys to users independently. In this work ,it has been proposed a novel access control heterogeneous framework to address the low efficiency and single-point performance bottleneck for public cloud storage. It proposes a robust and efficient heterogeneous framework with single CA(Central Authority) and multiple AAs (Attribute Authorities) for public cloud storage. The heavy load of user legitimacy verification is shared by multiple AAs, each of which manages the universal attribute set and is able to independently complete the user legitimacy verification, while CA is only responsible for computational tasks which generate secret keys for legitimacy verified users. To enhance security, we also propose an auditing mechanism to detect which AA (Attribute Authority) has incorrectly or maliciously performed the legitimacy verification procedure.

II LITERATURE REVIEW

"Zhangjie Fu, Kui Ren, Enabling personalized search over encrypted outsourced data with efficiency improvement 2015 IEEE." In cloud computing, searchable encryption scheme over outsourced data is a hot research field. However, most existing works on encrypted search over outsourced cloud data follow the model of one size fits all and ignore personalized search intention. Moreover, most of them support only exact keyword search, which greatly affects data usability and user experience. So how to design a searchable encryption scheme that supports personalized search and improves user search experience remains a very challenging task. In this paper, for the first time, we study and solve the problem of personalized multi keyword ranked search over encrypted data (PRSE) while preserving privacy in cloud computing. With the help of semantic ontology Word Net, we build a user interest model for individual user by analyzing the users search history, and adopt a scoring mechanism to express user interest smartly. To address the limitations of the model of one size fit all and keyword exact search, we propose two PRSE schemes for different search intentions. Extensive experiments on real-world dataset validate our analysis and show that our proposed solution is very efficient and effective [1].

"Zhangjie Fu, Xingming Sun and Sai Ji, Towards efficient content-aware search over encrypted outsourced data in cloud IEEE INFOCOM 2016" With the increasing adoption of cloud computing, a growing number of users outsource their datasets into cloud. The datasets usually are encrypted before outsourcing to preserve the privacy. However, the common practice of encryption makes the effective utilization difficult, for example, search the given keywords in the encrypted datasets. Many schemes are proposed to make encrypted data searchable based on keywords. However, keyword-based search schemes ignore the semantic representation information of users retrieval, and cannot completely meet with users search intention. Therefore, how to design a content-based search scheme and make semantic search more effective and context-aware is a difficult challenge. In this paper, we proposed an innovative semantic search scheme based on the concept hierarchy and the semantic relationship between concepts in the encrypted datasets. More specifically, our scheme first indexes the documents and builds trapdoor based on the concept hierarchy. To further improve the search efficiency, we utilize a tree-based index structure to organize all the document index vectors. Our experiment results based on the real world datasets show the scheme is more efficient than previous scheme. We also study the threat model of our approach and prove it does not introduce any security risk [3].

"Yingjie Xue, Jianan Hong,Wei Li and Kaiping Xue, LABAC: A locationaware attribute-based access control scheme for cloud storage 2016 IEEE" Data access control is a challenging issue in cloud storage. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a potential cryptographic technique to address the above issue, which is able to enforce data access control based on users permanent characteristics. However, in some scenarios, access policies are associated with users temporary conditions (such as access time and location) as well as their permanent ones. CP-ABE cannot deal with such situations commendably. In this paper, we focus on the scenario where users access privilege is determined by their attributes, together with their locations. To cope with this data access control requirement, we propose a location-aware attribute-based access control mechanism (LABAC) for cloud. In LABAC, we uniquely integrate CP-ABE with location trapdoors to make up access policies. In this way, data owners can flexibly combine both users attributes and locations to implement a fine-grained control of their data. A competitive advantage of LABAC is that it requires no any additional revocation mechanisms to revoke location-aware access privilege when user location changes. Security and performance analysis are presented which show the security and efficiency of LABAC for practical implementations [9].

Even though the definitions and constructions of different CPABE schemes are not always accurate, the uses of the access structure in Encrypt and Decrypt algorithms are nearly the same. Here we adopt the definition and construction from [6, 10].

A CP-ABE scheme consists of four algorithms: Setup, Encrypt, Key Generation (KeyGen), and Decrypt.

Setup(λ, U) $\rightarrow$ (PK,MSK). The setup algorithm takes the security parameter λ and the attribute universe description U as the input. It outputs the public parameters PK and a master secret key MSK.

Encrypt(PK,M,A) $\rightarrow$ CT. The encryption algorithm takes the public parameters PK, a message M, and an access structure A as input. The algorithm will encrypt M and produce a ciphertext CT such that only a user whose attributes satisfies

the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.

KeyGen(*MSK, S*) → *SK*. The key generation algorithm takes the master secret key *MSK* and a set of attributes *S* as input. It outputs a secret key *SK*.

Decrypt(*PK,CT, SK*)→*M*. The decryption algorithm takes the public parameters *PK*, a ciphertext *CT* which contains an access policy A, and a secret key *SK* as input, where *SK* is a secret key for a set *S* of attributes. If the set *S* of attributes satisfies the access structure A, the algorithm will decrypt the ciphertext and return a message *M*.

In Cloud computing searchable encryption is a challenging task. However, most of the existing works follow the model of "one size fits all" and ignore personalized search over outsourced encrypted data. So PRSE framework solves the problem of personalized multi-keyword ranked search over encrypted data by preserving security of the system in cloud computing. This framework builds user interest model for every user with the help of semantic ontology WordNet by analysis user's search history and by adopting a scoring mechanism to express user interest smartly. This framework supports both personalized multi-keyword ranking search and query extension.[1]

This framework involves three entities: the data owner (owner), the data user (user) and the cloud server (server). There exists a user interest model stored in the user side. User's interest model is built upon user's search history since long time. Using WordNet, it records access frequency of both query keywords and their related keywords. Different access frequency of keywords as different priority reflects different importance of keywords with respect to user's interest. In order to start with search for files of interest, data user has to produce a search request first. And then query reformulation will be carried out by user interest model which achieves user keyword priority of query terms. After this encrypted search query through search control mechanism will be sent to the cloud server. Upon receiving search query from authorized user, the cloud server will conduct some designated search over the index and returns relevant encrypted documents which have been ranked by some ranking criteria (scoring mechanism) by cloud server. Here cloud server is the single authority who does searching, indexing and ranking of relevant documents and sends back to the user.

In DAC-MACS(Data Access Control For Multi-Authority Cloud Storage) framework a multi authority CP-ABE scheme is used where each attribute authority maintains disjoint attribute set which is proposed to provide efficient decryption and efficient attribute revocation method for it, which is then applied to get effective data access control with multiple attribute authorities in cloud storage system. This framework consists of five entities: a Certificate Authority(CA), the Attribute Authorities(AAs),the cloud server(server),the data owners(Owner),the data users(users) [10].

The CA is trusted Certificate Authority in the system who initializes the system and does registration of AAs and users. For every legal user CA assign a global unique user identity, legal user means user who has been authenticated with the system.CA also generates a pair of global secret key and global public key for this user. AA is an attribute authority who independently issues, revokes and updates user's attributes according to their identity in the domain. Every attribute is associated with single AA and each AA maintains arbitrary number of attributes. Each AA generates public attribute key for each attribute it manages and secret key for the user who possesses same attributes. The cloud server stores the encrypted data of the owner and allows data access to legal users. It generates cipher text decryption token using secret keys generated by AAs for the users. Using that decryption token user can decrypt the cipher text. The server can generate correct decryption token only when the attributes satisfy the access policy defined in the cipher text. To get cipher text decryption token user has to submit global public key and secret key generated by some AAs to the server .After server generates decryption token, using this token along with global secret key user can decrypt the cipher text. The server does cipher text update when attribute revocation happens. Every owner divides his/her data into several components depending on logical granularities and encrypts each component with content keys using symmetric key algorithms. These content keys are encrypted by the access policy defined by data owner over attributes from different attribute authorities. Then the owner sends the encrypted data along with the cipher text to the server. Thus it provides efficient decryption method using token based decryption.

It also provides efficient attribute revocation method in multi-authority CP-ABE scheme which facilitates both forward security and backward security. It is efficient means it occurs with less communication and less computation cost. The revoked users can't decrypt the new ciphertext
as it needs revoked attributes to decrypt. This is called backward security. The new user can also decrypt the earlier published data encrypted with earlier public keys, if it has sufficient attributes. This is called forward security.

III SYSTEM ARCHITECTURE

We propose a novel heterogeneous framework to remove the problem of single-point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism. Our framework employs multiple attribute authorities to share the load of user legitimacy verification. Meanwhile, in our scheme, a central authority is introduced to generate secret keys for legitimacy verified users.

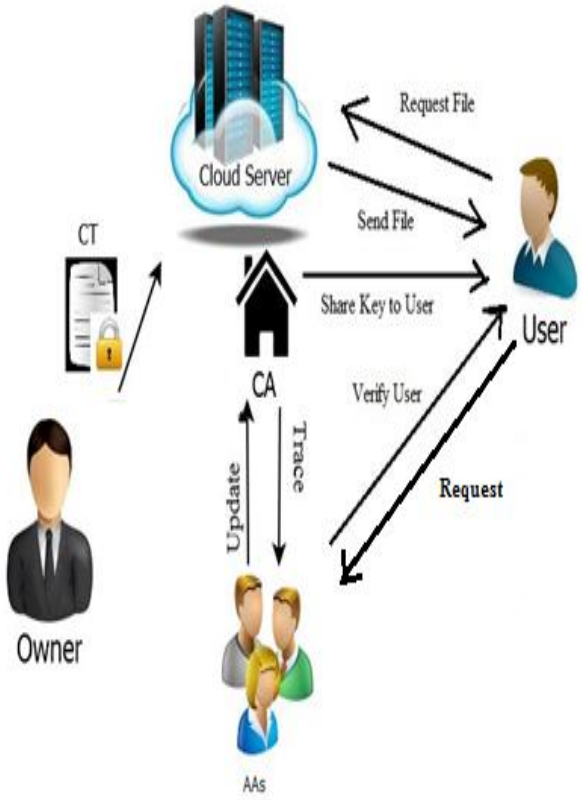

Figure1: System Architecture

Methodology

1) Data Owner

Data owner encrypts the data with symmetric key algorithm. He/She defines the access policy over an attribute set and then encrypts the symmetric key under the policy according to the public keys obtained by CA. Data owner is verified for its legitimacy during registration and data is also verified before uploading.

2) User

The data user (consumer) is assigned a global user identity Uid by CA. It can get any interested encrypted data from the cloud and the user can decrypt the encrypted data if and only if its attribute set satisfy the access policy.

3) Central Authority (CA)

It is the administrator of the entire system. It helps in system construction by setting up system parameters and generating public key for attribute of universal attribute set. It generates unique ids for AAs and users after registration. It generates secrete keys for legitimacy verified users. It has capacity to trace which AA has maliciously verified a user.

4) Attribute Authorities (AAs)

The attribute authorities (AAs) manage the whole attribute set individually so it can perform legitimacy verification of any user independently. AAs verify users legitimate attributes and generates intermediate key to assist CA to generate secret keys.

5) Cloud Server

Cloud servers provide public platform for data owners to store and share their encrypted data. Encrypted data can be freely downloaded by any user.

Advantages

- ✓ The Proposed System is efficient and scalable.
- ✓ Data confidentiality.
- ✓ Provides Data Security

V CONCLUSION AND FUTURE WORK

It has been proposed a new heterogeneous framework to eliminate the single point performance bottleneck and increase the efficiency of the existing CP-ABE schemes. By effectively reformulating CP-ABE cryptographic technique into this novel framework, the proposed scheme provides a fine-grained, robust and efficient access control with one-CA/multi-AAs for public cloud storage. This scheme employs multiple AAs to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of users requests. It has been proposed an auditing method to trace an attribute authority's potential misbehavior. It has been conducted detailed security and performance analysis to verify that this scheme is secure and efficient. The security analysis shows that the scheme could effectively resist to individual and colluded malicious users, as well as the honest-but-curious cloud servers.

The system can be further improved by increasing the security, as it is mentioned that CA is assumed to be trustworthy, however we can check its behavior and take action if there is any discrepancy. This will surely make the system more secure and efficient.

REFERENCES

1. Zhangjie Fu, Kui Ren, "Enabling personalized search over encrypted outsourced data with efficiency improvement" 2015 IEEE.
2. Zhangjie Fu, Xingming Sun and Sai Ji, "Towards efficient content-aware search over encrypted outsourced data in cloud" IEEE INFOCOM 2016
3. Kaiping Xue, "A dynamic secure group sharing framework in public cloud computing" 2013 IEEE.
4. Attribute-based access to scalable media in cloud-assisted content sharing
5. Junbeom Hur "Improving security and efficiency in attribute based data sharing" 2013 IEEE.
6. J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.
7. Jianan Hong, Kaiping Xue "TAFC: Time and attribute factors combined access control on time sensitive data in public cloud" 2015 IEEE

8. Yingjie Xue, Jianan Hong, Wei Li and Kaiping Xue, "LABAC: A location-aware attribute-based access control scheme for cloud storage" 2016 IEEE
9. K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS:Effective data access control for multi-authority cloud storage systems" 2013 IEEE
10. Jianwei Chen and Huadong Ma "Efficient decentralized attribute based access control for cloud storage with user revocation" 2014 IEEE
11. Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage" 2015 IEEE.