TMACS: A Robust and Verifiable Threshold Multi Authority Access Control System in Public Cloud Storage.

[1] Bhuvanashree Rao, [2]KV Manuja KJ, [3]Nagendra YC,[4]Sahana GR
[1]UG Scholar , Dept. of CSE, BGSIT B G Nagar India
[21]UG Scholar , Dept. of CSE, BGSIT B G Nagar India
[31]UG Scholar , Dept. of CSE, BGSIT B G Nagar India

ABSTRACT-Cloud computing is a type of internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. Despite many advantages of cloud storage, there still remain various challenging obstacles, among which, privacy and security of users' data have become major issues, especially in public cloud storage. Data is no longer in data owner's trusted domains and the data owner cannot trust on the cloud server to conduct secure data access control. Therefore, the secure access control problem has become a critical challenging issue in public cloud storage. Attribute-based Encryption (ABE) is regarded as one of the most suitable schemes to conduct data access control in public clouds. ABE system, a user's keys and cipher texts are labelled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. ABE schemes involve only one authority to maintain the whole attribute set, which can bring a single-point bottleneck on both security and performance. Some multi-authority schemes are proposed, in which multiple authorities separately maintain disjoint attribute subsets. So that, the single-point bottleneck problem remains unsolved. With the help of this project, 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 sharing, the master key can be shared among multiple authorities, and a legal 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.

Keyword: CP-ABE, Threshold secret sharing, Multi-authority, Public cloud storage, Access control.

I. INTRODUCTION

A data owner stores his/her data in trusted servers, which are generally controlled by a fully trusted administrator. However, in public cloud storage systems, the cloud is usually maintained and managed by a semi-trusted third party (the cloud provider). Data is no longer in data owner's trusted domains and the data owner cannot trust on the cloud server to conduct secure data access control. Therefore, the secure access control problem has become a critical challenging issue in public cloud storage, in which traditional security technologies cannot be directly applied.

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 Cipher text-Policy Attribute-based Encryption(CP-ABE). In KP- ABE schemes, decrypt keys are associated with access structures while cipher texts are only labelled with special attribute sets. 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. In existing CP-ABE schemes 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. 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. To solve this problem proposal is a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS in which multiple authorities jointly manage a uniform attribute set. In TMACS, taking advantage of (t; n) threshold secret sharing, the master key can be shared among multiple authorities, and a legal 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. To the best of knowledge, first try to address the single point bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

II. SYSTEM MODEL

Proposed System Framework and basic protocol flow In the above proposed system framework there are five entities:

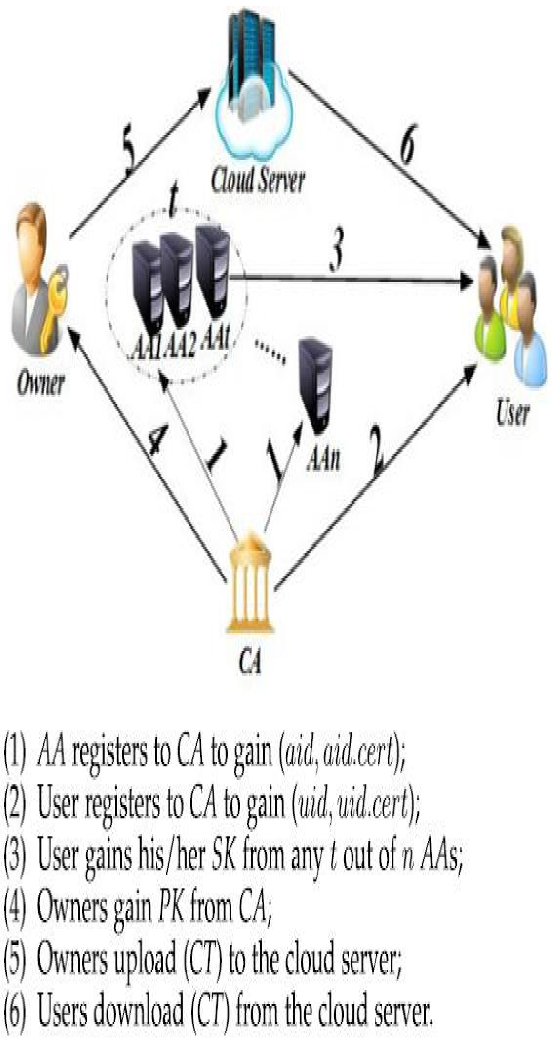
Certificate authority (CA): The certificate authority is a global trusted entity in the system that is responsible for the construction of the system by setting up system parameters and attribute public key (PK) of each attribute in the whole attribute set. CA accepts users and AAs' registration requests 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.

Multiple attribute authorities (AAs): 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. That is to say, no communication among AAs is needed in the phase of users' secret key generation.

Data owners (Owners): The data owner (Owner) encrypts his/her file and defines access policy about who can get access to his/her data. First of all, each owner encrypts his/her data with a symmetric encryption algorithm like AES and DES. Then the owner formulates access policy over an attribute set and encrypts the symmetric key under the policy according to attribute public keys gained from CA. Here, the symmetric key is the key used in the former process of symmetric encryption. After that, the owner sends the whole encrypted data and the encrypted symmetric key to store in the cloud server. However, the owner doesn't rely on the cloud server to conduct data access control. Data stored in the cloud server can be gained by any data consumer. Despite all this, no data consumer can gain the plaintext without the attribute set satisfying the access policy.

Data Users: The data consumer (User) is assigned with a global user identity uid from CA, and applies for his/her secret keys from AAs with his/her identification. The user can freely get the cipher text that he/she is interested in from the cloud server. He/She can decrypt the encrypted data if and only if his/her attribute set satisfies the access policy hidden inside the encrypted data.

The cloud server: 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. The encrypted data stored in the cloud server can be downloaded freely by any data consumer.



III. PREVIOUS WORK

In previous work proposed an Attribute-based Encryption (ABE) which is 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. An Attribute-based Encryption (ABE) divided into two categories such as Key-Policy Attribute-based Encryption (KP- ABE) and Cipher text-Policy Attribute-based Encryption (CP-ABE). Compared with KP-ABE, CP-ABE is a preferred choice for designing access control for public cloud storage. In existing CP- ABE schemes 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. 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.

DISADVANTAGES OF PREVIOUS WORK :

1) In single authority CP-ABE scheme, only one authority responsible for attribute management and key distribution. 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 subset to decrypt the specific encrypted data. Therefore this only-one-authority scenario can bring a single- point bottleneck on both security and performance.

2) In multi-authority CP-ABE scheme, the adversary can obtain private keys of specific attributes by compromising specific one or more authorities. Therefore the single point bottleneck on performance and security is not yet solved.

IV. PROPOSED METHODOLOGY

A new concept called 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. In TMACS, taking advantage of (t; n) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. 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 knowledge, first try to address the single point bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

V. CONCLUSION

Here proposed a new concept called 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. In TMACS, taking advantage of (t; n) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. 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 knowledge, first try to address the single point bottleneck on both security and performance in CPABE access control schemes in public cloud storage.

VI. FUTURE SCOPE

In Future, based on efficiently combining the traditional multi-authority scheme with TMACS, we also construct a hybrid scheme that is more suitable for the real scenario, in which attributes come from different authority-sets and multiple authorities in an authority-set jointly maintain a subset of the whole attribute set. This enhanced scheme addresses not only attributes coming from different authorities but also security and system-level robustness. How to reasonably select the values of (t; n) in theory and design optimized interaction protocols will be addressed in our future work.

REFERENCES

1) R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. 14th ACMConf. Comput. Commun. Security, 2014, pp. 195–203.

2) Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," IEEE Trans. Multimedia, vol. 15, no. 4, pp. 778–788, Jun. 2013.

3) Z. Wan, J. Liu, and R. Deng, "Hasbe: A hierarchical attributebased solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.

4) J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2014.

5) K. Yang and X. Jia, "Attributed-based access control for multiauthority systems in cloud storage," in Proc. IEEE 32nd Int. Conf. Distrib. Comput. Syst., 2012, pp. 536–545.

6) K. Yang and X. Jia, "Expressive, efficient and revocable data access control for multi-authority cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, Jul. 2013. 304–307.

7) K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective data access control fr multi-authority cloud storage systems," in Proc. 32nd IEEE Int. Conf. Comput. Commun., 2013, pp. 2895–2903.

8) H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multiauthority attribute based encryption without a central authority,"Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2011