ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Time and Attribute Factors Combined Access Control on Time-Sensitive Data in Public Cloud

A Prashanth
B.Tech Scholar,
Department of Computer Science & Engineering,
Siddhartha Institute of Engineering and Technology,
Vinobha Nagar, Ibrahimpatnam, Hyderabad,
Telangana 501506, India.

M Swetha
Assistant Professor,
Department of Computer Science & Engineering,
Siddhartha Institute of Engineering and Technology,
Vinobha Nagar, Ibrahimpatnam, Hyderabad,
Telangana 501506, India.

Abstract

The new paradigm of outsourcing data to the cloud is a double-edged sword. On one side, it frees up data owners from the technical management, and is easier for the data owners to share their data with intended recipients when data are stored in the cloud. On the other side, it brings about new challenges about privacy and security protection. To protect data confidentiality against the honest-but-curious cloud service provider, numerous works have been proposed to support fine-grained data access control. However, till now, no efficient schemes can provide the scenario of fine-grained access control together with the capacity of time-sensitive data publishing. In this paper, by embedding the mechanism of timed-release encryption into CP-ABE (Ciphertext- Policy Attribute-based Encryption), we propose TAFC: a new time and attribute factors combined access control on time sensitive data stored in cloud. Extensive security and performance analysis shows that our proposed scheme is highly efficient and satisfies the security requirements for time-sensitive data storage in public cloud.

INTRODUCTION

Cloud storage service has significant advantages on both convenient data sharing and cost reduction. However, this new paradigm of data storage brings about new challenges about data confidentiality protection. Data are no longer in data owner's trusted domain, and he/she cannot trust the cloud server to conduct secure data access control. Therefore, the secure access control problem has become a challenging issue in cloud storage.

There have been numerous works [1–5] on privacy preserving data sharing in cloud based on various cryptographic primitives, in which the schemes [1–3] based on CP-ABE [6] attract extensive attentions, since they can guarantee data owner fine-grained and flexible access control of his/her own data. However, these schemes determine user's access privilege only based on his/her inherent attributes without any other critical aspects, such as the time factor. In reality, the time factor usually plays an important role in dealing with time sensitive data [7] (e.g. to publish a latest electronic magazine, to expose a company's future business plan).

When uploading time-sensitive data to the cloud, the data owner may want different users to access the content after different time. However, to the best of our knowledge, existing CP-ABE based schemes cannot meet such requirement. To tackle the above issue of timed release, it is necessary to introduce an effective scheme, which will not release the data access privilege to intended user until corresponding predefined time. A trivial solution is to leave data owners to manually release the time-sensitive data: The owner uploads the encrypted data under different policies at each release time, thus intended users cannot access the data until the corresponding time arrives. However, such solution restricts the owner to be online to repeatedly upload the different encryption versions of the same data, which makes the data owner in a heavy trouble.

From the perspective of cryptography, the goal of timed release can be achieved by Timed-Release Encryption (TRE). Rivest et al. [8] have proposed an effective TRE scheme, and it has been subsequently introduced into different aspects, such as searchable encryption [9], proxy re-encryption [10], conditional oblivious transfer [11]. In a TRE-based system, a trust time agent, rather than data owner, can uniformly release the access privilege at each predefined time. Androulaki et al. [12] have designed an approach to realize time-sensitive data access control in cloud. Whereas, this approach lacks fine granularity, which may leave the data owners an unbearable burden in a large-scale system. Fan et al. [13] have proposed timed-release predicate encryption for cloud computing. In their scheme, each data file can be labelled with only one release time point, which cannot release the access privilege of one file to different intended users at different time.

How to achieve the capacity of both timed-release and fine-grained access control in cloud storage? A direct but naive method is to handle time as an attribute [12]. However, unbearable number of time-related keys will be issued to each user at each corresponding time, and this will bring about heavy overhead on both computation and communication. In existing literatures, Qin et al. [10] have made a preliminary attempt to integrate time with attributes. It only addresses the issue that the attributes' life period of each user may be limited by time. However, a more practical scheme is that: each user with different attribute sets will have different release time for the same data file. Thus, the scheme in [10] cannot meet this important requirement.

In this paper, we propose an efficient time and attribute factors combined access control scheme for time-sensitive data in public cloud, named TAFC. Our scheme has two important capacities: on one side, it inherits the property of fine granularity from CP-ABE; on the other side, by introducing the trapdoor mechanism, it further has the feature of timed release from TRE. In our scheme, the introduced trapdoor mechanism is only related to the time factor, in which only one corresponding secret should be published at each time to expose the related trapdoors. This makes our scheme highly efficient, with only little extra overhead added to the original CP-ABE based scheme.

The main contributions of this paper can be summarized as follows:

1) To the best of our knowledge, this paper is the first that proposes two factors(time and attributes) combination based access control scheme I cloud storage,which can simultaneously achieve the features of fine granularity and timed release.

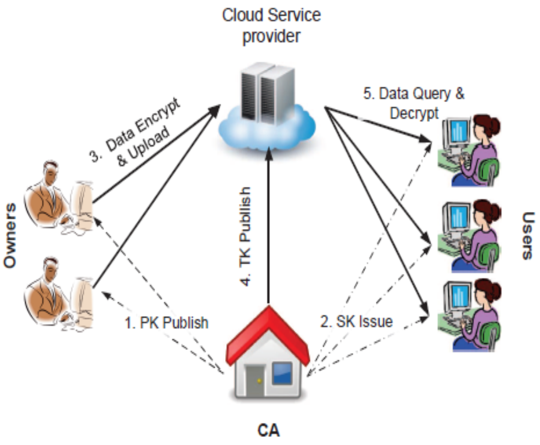

Fig 1: TAFC Architecture and Operations

2) We design an effective architecture to realize our scheme, in which we redesign an entity (the central authority, CA) to be responsible for the timed-release function. Besides distributing attribute-associated private keys, CA only needs to periodically publish universal time-related tokens to release access privileges. Such architecture occupies only a small amount of cost to provide our required access control scheme, which is reasonable and worthy.

3) For the function of timed release, there is no use of a secure tunnel between CA and the data owner. Thus, the additional overhead is lightweight.

SYSTEM ANALYSIS

EXISTING SYSTEM

The conventional approach to address privacy in this context is to encrypt sensitive data before outsourcing it and run all computations on the client side. However this imposes unacceptable client-overhead, as data must continuously be downloaded, decrypted, processed, and securely re-uploaded. Many applications cannot cope with this overhead, particularly online and mobile applications operating over very large datasets such as image repositories with CBIR services. A more viable approach would be to outsource computations and perform operations over the encrypted data on the server side. Existing proposals in this domain remain largely unpractical, namely those requiring fully homomorphism encryption, which is still computationally too expensive.

PROPOSED SYSTEM

Cloud storage service has significant advantages on both convenient data sharing and cost reduction. However, this new paradigm of data storage brings about new challenges about data confidentiality protection. Data are no longer in data owner's trusted domain, and he/she cannot trust the cloud server to conduct secure data access control. Therefore, the secure access control problem has become a challenging issue in cloud storage.

PROPOSED SYSTEM ALGORITHMS

- Encryption.
- Decryption
- Security Hash Algorithm.

ALGORITHM

Encryption Algorithm:

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would produce no useful result. In encryption, a key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption**.**

Security Hash Algorithm:

The Secure Hash Algorithm is a family of cryptographic hash functions

Architecture Diagram

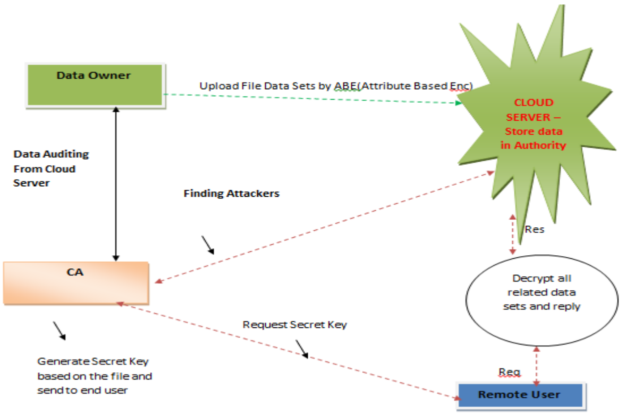
Data Owner
Upload File Data Sets by ABE(Attribute Based Enc)
CLOUD SERVER – Store data in Authority
Data Auditing From Cloud Server
Finding Attackers
Res
CA
Decrypt all related data sets and reply
Request Secret Key
Generate Secret Key based on the file and send to end user
Req
Remote User

Fig.2.data secure hash algorithm

ABE --- Attribute Based Encryption

Data Sets --- Personal Details, Medical Report, Medical Summary

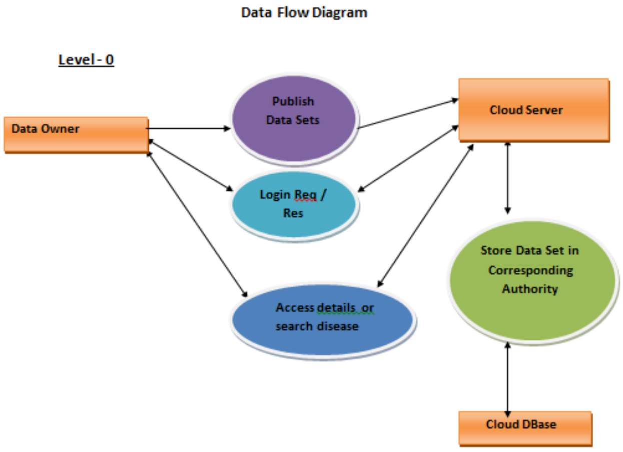

Fig.3.data flow diagram for level zero (data Owner)

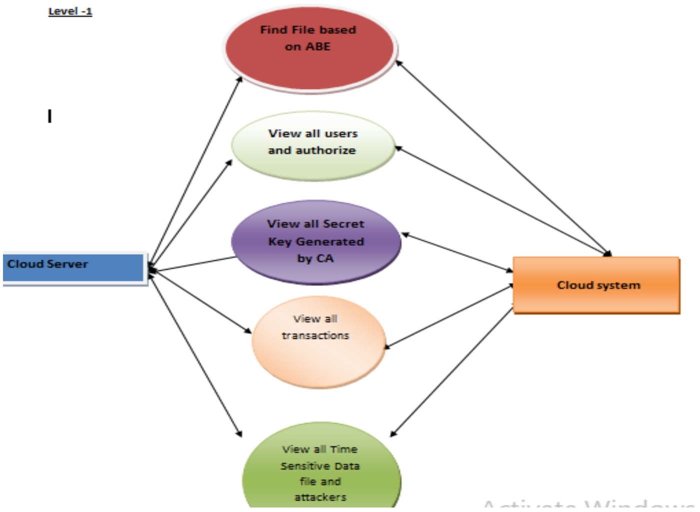
Level -1
Find File based on ABE
View all users and authorize
View all Secret Key Generated by CA
Cloud Server
Cloud system
View all transactions
View all Time Sensitive Data file and attackers

Fig.4.cloud chart

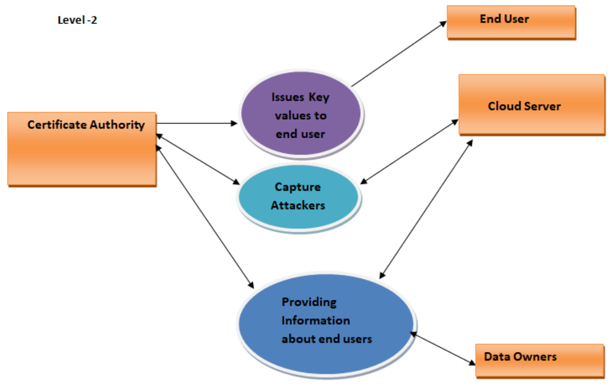

Fig.5.user flow chart

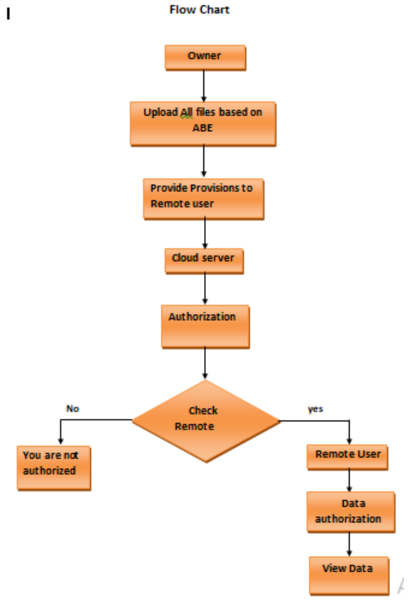

Fig.6.flow chart for owner to user server

IMPLEMENTATION

Data Owner

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

Cloud Server

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. It is responsible for authorizing all end users.

Certificate Authority

CA **who** is trusted to store verification parameters and offer public query services for these parameters such as generating secret key based on the file and send to the corresponding end users. It is responsible for capturing the attackers.

Data Consumer/End User

In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the Data owner and the Data users are controlled by the data owner only. Users may try to access data files either within their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. He is sending request to CA to generate secret key and CA will generate the skey and send to corresponding end user.

Attacker (Unauthorized User)

Attacker adds the malicious data to a block in cloud server. Then the Unauthorized user will considered as a attacker.

CONCLUSION

This paper aims at fine-grained access control for timesensitive data in cloud storage. One challenge is to simultaneously achieve flexible timed release and fine granularity with lightweight overhead, which is not provided in related work. In this paper, we propose a scheme to achieve this goal. Our scheme seamlessly incorporates the concept of timed-release encryption to the architecture of ciphertext-policy attributebased encryption. With a suit of proposed mechanisms, this scheme provides data owners with the capability to flexibly release the access privilege to different users at different time, according to a well-defined access policy over attributes and release time. The analysis shows that our scheme can protect the confidentiality of time-sensitive data, with a lightweight overhead on both CA and data owners, thus well suits the practical large-scale access control system for cloud storage.

REFERENCES

[1] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754, 2012.

[2] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1790–1801, 2013.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[4] Z. Zhou, H. Zhang, Q. Zhang, Y. Xu, and P. Li, "Privacypreserving granular data retrieval indexes for outsourced cloud data," in Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM2014), pp. 601–606, IEEE, 2014.

[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," in Proceedings of the 2011 IEEE Global Communications Conference (GLOBECOM2011), pp. 1–5, IEEE, 2011.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy\ attribute-based encryption," in Proceedings of the 28th IEEE Symposium on Security and Privacy (S&P2007), pp. 321–334, IEEE, 2007.

[7] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 191–233, 2001.

[8] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," tech. rep., Massachusetts Institute of Technology, 1996.

[9] K. Yuan, Z. Liu, C. Jia, J. Yang, and S. Lv, "Public key timed-release searchable encryption," in Proceedings of the 2013 Fourth International Emerging Intelligent Data and Web Technologies (EIDWT2013), pp. 241–248, IEEE, 2013.

[10] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences, vol. 258, no. 3, pp. 355–370, 2014.

[11] L. Xu, F. Zhang, and S. Tang, "Timed-release oblivious transfer," Security and Communication Networks, vol. 7, no. 7, pp. 1138– 1149, 2014.

[12] E. Androulaki, C. Soriente, L. Malisa, and S. Capkun, "Enforcing location and time-based access control on cloud-stored data," in Proceedings of the 2014 IEEE 34th International Distributed Computing Systems (ICDCS2014), pp. 637–648, IEEE, 2014.

[13] C.-I. Fan and S.-Y. Huang, "Timed-release predicate encryption and its extensions in cloud computing," Journal of Internet Technology, vol. 15, no. 3, pp. 413–426, 2014.

[14] X. Zhu, S. Shi, J. Sun, and S. Jiang, "Privacy-preserving attribute-based ring signcryption for health social network," in Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM2014), pp. 3032–3036, IEEE, 2014.

[15] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in

Cryptology (CRYPTO2001), pp. 213–229, Springer, 2001.

Author Details

Prashanth is a student of B.Tech fourth year in Computer Science from Siddhartha Institute of Engineering and Technology. His subjects of interest are Data mining and Android.

M.Swetha, M.Tech, working as Asst. Prof at CSE Dept in Siddhartha Institute of Engineering and Technology, Ibrahimpatnam. Her area of interest is Cloud Computing, Database Management System and Big Data.