Combined Access Control of Time and Attributes for Time Sensitive Data in Cloud

[1]K. Seema Sri Vatsavi, [2]Dr. Ch. Niranjan Kumar, [3]Dr. Prashanta Kumar Sahoo
[1,2,3]Sreenidhi Institute of Science & Technology, Hyderabad, India

Abstract
The brand-new pattern of deploy data to the cloud is a two-edged sword. On the one hand, it enables data owners to share their information with desired individuals. On the various other hand, it posses brand-new is difficulties on personal privacy and also security protection. To protect information secretness versus the honest-but-curious cloud company, many jobs have actually been suggested to sustain great grained data access control. Nevertheless, till currently, no approaches can sustain both fine-grained accessibility control and also time-sensitive information posting. In this paper, by incorporating timed-release encryption right into CP-ABE (Ciphertext-Policy Attribute-based Encryption), we recommend a brand-new time and also attribute aspects consolidated gain access to control on time-sensitive information for public cloud storage (called TAFC).

Keywords
Cloud Storage, Time-sensitive Data, Access Control, Fine Granularity

I. Introduction

Ciphertext-policy attribute-based encryption (CP-ABE) [5] is a helpful cryptographic technique for data access control in cloud storage space [6-- 8] All these CP-ABE based plans make it possible for data owners to recognize fine-grained and also versatile gain access to control by themselves information. Nonetheless, CP-ABE figures out individuals' accessibility opportunity based just on their integral features with no various other important elements, such as the moment aspect. Actually, the moment variable typically plays a crucial duty in taking care of time-sensitive information (e.g. to release a most current digital publication, or to subject a firm's future organization strategy). In these situations, both the system of gain access to advantage timed launching and also fine-grained gain access to control ought to be with each other considered. Allow us to take the venture information direct exposure, for example, A firm generally prepares some essential apply for various designated individuals, as well as these customers can obtain their accessibility opportunity at various time factors. As an example, the future strategy of this firm might have some service tricks. Hence at a very early time, the accessibility advantage can be launched to the Chief Executive Officer just. After that, the supervisors of some appropriate divisions can obtain accessibility benefit at a later time factor when they take duty for the strategy implementation. Finally, various other workers in some details divisions of the firm can access the information to assess the efficiency of this venture strategy. When posting time-sensitive information to the cloud, the information proprietor desires various individuals to access the material after various time factors. To the outsourced information storage space, CP-ABE can identify various customers as well as give fine-grained accessibility control. Nonetheless, to our finest understanding, these systems can not sustain progressive gain access to benefit launching.

To recognize the feature of timed launching, it is essential to present a reliable system, which will certainly not launch the information accessibility opportunity to desired customers still getting to pre-specified time factors. An unimportant service is to allow data owners by hand launch the time-sensitive information: The proprietor submits the encrypted information under various plans at each launching time such that the designated individuals cannot access the information till the matching time shows up. Nonetheless, this service compels the proprietor to repetitively publish the various encryption variations of the exact same information, which places unneeded as well as hefty problem on the information proprietor. In this paper, we suggest a reliable time and also attribute elements consolidated gain access to control system, called TAFC, for time-sensitive information in public cloud. Our plan has 2 crucial capacities: 1) It acquires the home of great granularity from CP-ABE; 2) By presenting the trapdoor system, it even more maintains the attribute of timed launch from TRE. Keep in mind that in TAFC, the presented trapdoor device is just pertaining to the moment variable, and also just one matching secret requirements to be released when revealing the relevant catch- doors. This makes our plan extremely effective, which just causes little expenses to the initial CP-ABE based plan.

II. Literature Survey

A. Title: Attribute Based Encryption for fined grained access control of encrypted data.
Author: Sahai and Waters, Year: 2008

As more sensitive data is shared and stored by third party sites on the internet, there will be a need to encrypt stored at these sites. ABE is a type of public key encryption in which the secret key of a user and the cipher text that are dependent on attributes. We develop a new cryptosystem for fine grained sharing of encrypted data that we call key policy ABE. In our cryptosystem ciphertext are labeled with sets of attributes and private keys are associated with access structures that control with cipher text a user is able to decrypt.

Instead of encrypting each part with keys of all recipients it is possible to encrypt only with attributes that match recipients.
Example: He may be a user, admin or manage.

B. Title: Identity based encryption
Author: Amit Sahai and Waters, year 2010

In identity based encryption we view an identity as a set of descriptive attributes it allows for a private key fro an identity to decrypt a cipher text encrypted with some identity.
If and only if both the identities matches the user cannot decrypt the key. it can be applied to enable encryption using biometric inputs as identities.
It reduces complexity.
It requires centralized server, it also requires server channel between sender and receiver.
Example: Fingerprint, photo etc.

C. Title: Key policy attribute based encryption
Author: Chan-ji wang,Jian-fa luo, year: 2012

Key policy attribute based encryption is an important class of ABE where ciphertext are labeled with sets of attributes and private keys are associated with access structures that control with cipher text a user is able to decrypt.
Includes a dummy attribute in every file is encrypted. Easy to deal with user revocation and for the cloud server to learn about users.

Example: If there is admin what are the responsibilities of admin weather to edit or add information.

D. Title: Time based proxy re encryption scheme for secure data sharing in cloud environment
Author: Q.liu,G.wang Year : 2014

A fundamental approach for secure data sharing in cloud environment is to let the data owner encrypt the data before outsourcing. It is combination of ABE and Proxy re encryption to delete the cloud service provider to execute re encryption. The data owner should be online to send the proxy re encryption keys to cloud service provider in a timely fashion to prevent the revoked user accessing the future data. It denotes the period of validity of the users access right. Then the data owner and the cloud service provider are required to share a root secret key in advance. It achieves stronger notion of security.

III. Existing System

Rivest proposed a practical TRE algorithm. In TRE based system we have both data owner and the trusted time agent.

Now a trusted time agent rather than data owner can constantly release access right at a particular time but it lacks fine grained access control.

Qin made an attempt to integrate time with attributes but it only address the problem that attributes life period is limited by time.

One requirement is that every user with different attribute set can have different releasing time points for same file.

Disadvantages

- The data owner cannot trust the cloud server to conduct secure data access control.
- Users cannot access the data until the corresponding time arrives.
- These methods lack fine grained access control .

IV. System Architecture

A. System and Security Model

The system architecture in this process consists of four entities.
Central Authority (CA), Data Owner (DO), Data Consumer (Users) and Cloud Service Provider (Cloud).

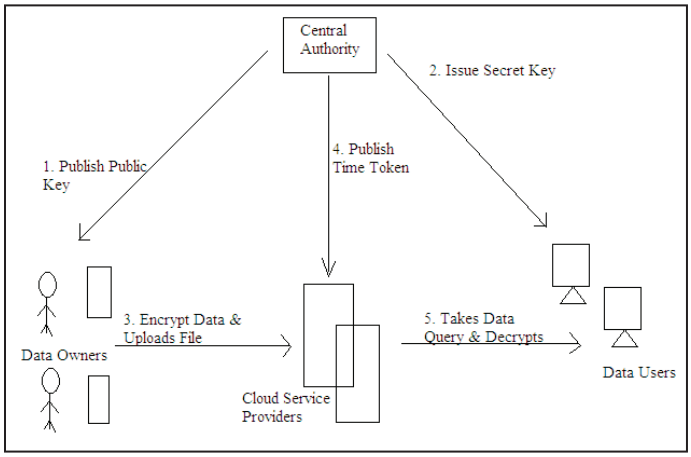

Fig. 1: Architecture

B. Operations

1. Central Authority

It acts as a time agent to maintain timed releasing function and distributes secret keys to every user security for the whole system is managed by central authority

(i). Data Owner

Based on attribute set it dislikes the access policy & time releasing points for each & every file. Then Encryption is based on policy decided.

2. Data User

Central Authority gives the security key to user, he can then decrypt the file if both the constraints are satisfied

- Should satisfy access policy based on attribute set
- Present access time is more than the given releasing time.

3. Cloud Service Provider

CSP is responsible for administration of cloud & cloud servers. Cloud executes access privilege releasing algorithm under control of CA.

As illustrated in fig. 1, the ciphertexts are transferred from proprietors to the cloud, and also individuals can quiz any type of ciphertexts. CA regulates the system with the complying with 2 procedures: 1) It releases security secrets to every customer, according to customer's attribute collection; 2) At each time factor, it releases a Time Token (TK), which is utilized to launch accessibility opportunity of information to individuals.

The data owner (Owner) chooses the entrance arrangement in light of a particular characteristic set and at least one discharging time focuses for each document, and afterward scrambles the record under the chose approach before transferring it. In detail, the proprietor scrambles his/her message for the reason that planned clients can decode it after an assigned time. From the security angle, TRE fulfills that: 1) Except the planned clients, nobody can get any data of the message 2) Even the proposed client can't get the plaintext of the message before the assigned discharging time.

The data consumer (User) is allocated a security key from CA. He/she can question any figure content put away in the cloud, yet can decode it just if both of the accompanying requirements are fulfilled: 1) His/her property set fulfills the entrance strategy; 2)

The present access time is later than the particular discharging time.

Cloud service provider (Cloud) incorporates the chairman of the cloud and cloud servers. The cloud attempts the capacity errand for different substances, and executes get to benefit discharging calculation under the control of CA. In our entrance control framework, the cloud is thought to be straightforward yet inquisitive. From one perspective, it offers solid stockpiling administration and effectively executes each calculation mission for different elements; then again, it might attempt to increase unapproved data for its own advantages.

V. Proposed System

A reliable time as well as attribute aspects mixed gain access to control plan, called TAFC, for time-sensitive information in public cloud has 2 vital capacities: 1) It acquire the building of great granularity from CP-ABE; 2) By presenting the trapdoor device, it additionally preserves the function of timed launch from TRE.

We need to assist exactly how to develop effective gain access to the framework for approximate accessibility benefit building and construction with both time and also attribute elements, particularly when gaining access to policy installs numerous gain access to advantage launching time factors.

In TAFC, the presented trapdoor system is just pertaining to the moment aspect, and also just one matching secret requirements to be released when subjecting the relevant trapdoors.This makes our system very effective.

Advantages

An efficient time and attribute factors combined access control scheme, named TAFC, for time-sensitive data in public cloud, has two important capabilities: 1) It obtains the property of fine granularity from CP-ABE; 2) By introducing the trapdoor mechanism, it further retains the feature of timed release from TRE. We should guide how to design an efficient access structure for arbitrary access privilege construction with both time and attribute factors, especially when an access policy embeds multiple access privilege releasing time points.
In TAFC, the introduced trapdoor mechanism is only related to the time factor, and only one corresponding secret needs to be published when exposing the related trapdoors. This makes our scheme highly efficient.

VI. Implementation

The Central Authority (CA) is capable to deal with the security assurance of the entire framework: It distributes framework parameters and conveys security keys to every client. Likewise, it goes about as a period operator to keep up the coordinated discharging function.CA is thought to be completely trusted, while clients could be malignant. CA is in charge of key dispersion and time token distributing. A malevolent client will attempt to unscramble the figure writings to acquire unapproved information by any conceivable means, incorporating intriguing with different indictive clients.

A. Algorithm

- Setup
- Key Generation
- Encryption
- Decryption
- Token Generation
- Trap door Exposure

Step 1: SETUP This is the first step in CP-ABE algorithm
Step 2: The setup algorithm takes only security parameter
Step 3: It outputs public parameters and also a master key

B. Encryption

Step 1: This is the second phase in CP-ABE algorithm
Step 2: We can use algorithms like AES, DES for encryption
Step 3: From setup phase it takes public parameter (PK) and input message that you want to encrypt (M) and access structure over the attributes.
Step 4: Now the algorithm will encrypt message and produce cipher text (CT)
Step 5: The produced cipher text can viewed by the person who passes attributes satisfies above access structure,

C. Key Generation

Step 1: Key generation algorithm takes master key (MK) as input
Step 2: It also takes attributes (S) that describes the key
Step 3: Now it outputs a private key (SK)

D. Decryption

Step 1: In this phase we use same algorithm that we used for encryption
Step 2: It takes as input public key, private key, attributes, cipher text and access structure
Step 3: Now if the set of attributes satisfies access structure message gets decrypted otherwise will return to message.

E. Token Generation

Step 1: It is nothing but an OTP or security alert
Step 2: At each point of time control authority generates and publicly publishes a time taken token tkt.

F. Trap Door Exposers

Step 1: Time trapdoor is generated by data owner when encrypting his data.
Step 2: When arriving at the realizing time point the cloud can obtain corresponding token published by central authority.
Step 3: Then the cloud server implements the procedure to expose trapdoor.

Fan et al. suggested timed-release predicate encryption for cloud computing. Nevertheless, each data can be classified with one factor, which cannot launch the gain access to benefit of one documents to various desired individuals at the various time.

Some looks into have actually additionally attempted to incorporate the systems of TRE and also CP-ABE, to give a versatile as well as fine-grained accessibility control for time-sensitive information. Zhu et al. recommended a temporal accessibility control system for cloud storage space, in which the cloud web server handles the moment as a global clock solution. Such building and construction cannot withstand the collusion between a cloud web server and also customers. In [6], the writers recommended time-domain gain access to the control system, in which gain access to control

takes both customer's attribute collection and also the accessibility time right into factor to consider. Nonetheless, it presents hefty added expenses: The authority requires to create upgrade tricks for all prospective attributes each time to carry out the time-related feature, as well as the computational complexity enhances with the quantity of included attributes.

VII. Results

Fig. 2: Edit/View/Time Details

Fig. 3: Owner Downloading File

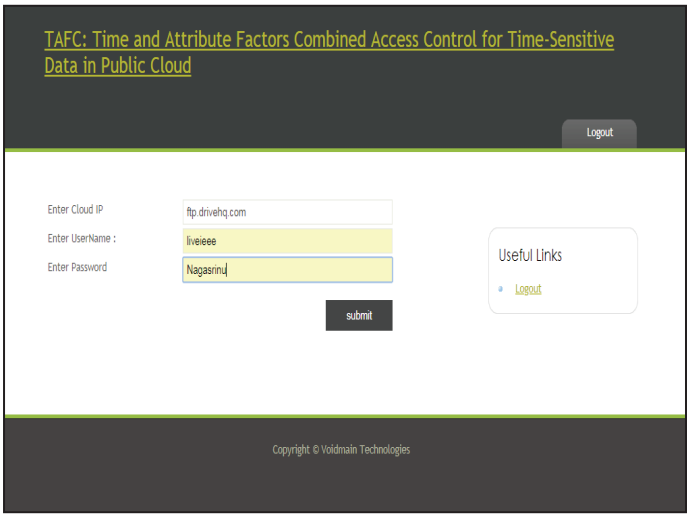

Fig. 4: Entering Cloud Details

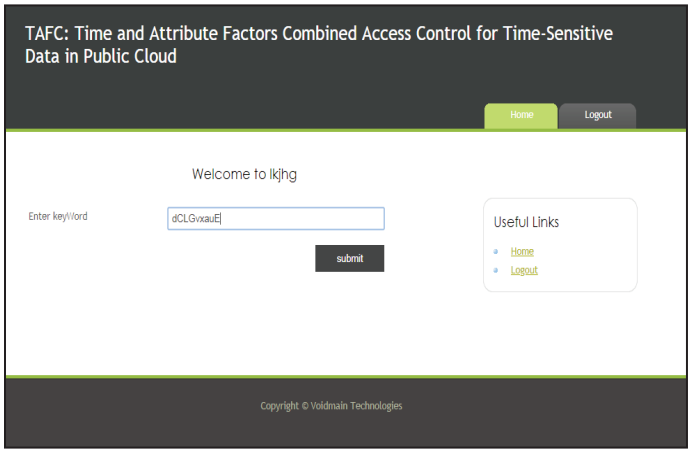

Fig. 5: Entering Keyword

VIII. Conclusion

In this paper, we suggested a strategy to complete the goal. Our strategy continually merges the suggestion of intended discharge encryption to the layout of cipher message strategy top quality based encryption. With a match of recommended systems, this strategy provides details owners with the ability to adaptably release the entry advantage to numerous customers at different time, based on a quite identified reach plan over high qualities as well as discharge time. We furthermore thought about accessibility technique rundown for all possible gain access to requirements of time fragile, via suitable plan of time trapdoors. The exam shows that our strategy can guard the category of time-touchy info, with light-weight expenses on both CA and also info owners. we suggest a brand-new time as well as attribute elements consolidated gain access to control on time-sensitive information for public cloud storage (called TAFC)..

References

[1] X. Zhu, S. Shi, J. Sun, S. Jiang,"Privacy- preserving attribute-based ring signcryption for health social network", In Proceedings of the 2014 IEEE.

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

[3] K. Yang, X. Jia, K. Ren, B. Zhang, 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. [Online] Available: https://doi.org/10.1109/TIFS.2013.2279531

[4] M. Li, S. Yu, Y. Zheng, K. Ren, 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. [Online] Available: https://doi.org/10.1109/TPDS.2012.97

[5] K. Yuan, Z. Liu, C. Jia, J. Yang, 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.

[6] J. Bethencourt, A. Sahai, B. Waters,"Cipher text policy attribute-based encryption", In Proceedings of the28th IEEE Symposium on Security and Privacy (S&P'07), pp. 321–334, IEEE, 2007.

[7] Z. Wan, J. Liu, 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.

[8] K. Yang, X. Jia, K. Ren, B. Zhang, R. Xie,"DACMACS: 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.

[9] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou,"Scalableand secure sharing of personal health recordsin cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 1, pp. 131–143, 2013.

[10] E. Bertino, P. A. Bonatti, E. Ferrari,"TRBAC: Atemporal role- based access control model," ACM Transactionson Information and System Security, Vol. 4, No. 3, pp. 191–233, 2001.