

Fine-Grained Access Control on Time-Sensitive Data Using Timed-Release Encryption with Ciphertext Attribute Based Encryption in Public Cloud

Shamili A¹, Shalini S², Prof. Geetha Megharaj³, Dr. K S Jagadeesh Gowda⁴

U.G. Student, Department of Computer Engineering, SKIT College, Bengaluru, Karnataka, India^{1,2}

Associate Professor, Department of Computer Engineering, SKIT College, Bengaluru, Karnataka, India³

Head of the Department, Department of Computer Engineering, SKIT College, Bengaluru, Karnataka, India⁴

ABSTRACT: In recent years one of the most important technique emerged in IT industry is cloud computing. This technology requires the data stored in cloud to be trusted, concept of security and privacy has increased. Most of the schemes proposed so far doesn't have flexibility in implementing complex access control. This paper achieves the flexibility and fine-grained access control in public cloud. We know that data security is an important factor in cloud which is to be concentrated because of data outsourcing and lack of trust in cloud servers. Another important pattern in cloud computing is the storage which acts as a service which provides great flexibility and also economic savings. The most important technique for data sharing in cloud is achieved by encrypting the data and issuing decryption keys by the data owners to the authorized users. One of the best technique used here is the CP-ABE (Ciphertext Policy Attribute Based Encryption) in which both keys and attributes are managed by a trusted authority. To protect the confidentiality of the data from the CSP (Cloud Service Provider) many schemes have been invented. However, there is no efficient scheme, which embeds fine-grained access control together with the time sensitive data. In this paper we combine both the time and attribute factors. By embedding the TRE (Timed-release Encryption) into CP-ABE, we propose "Fine-Grained Access Control on Time-Sensitive Data using Timed-Release Encryption with Ciphertext Attribute Based Encryption in Public Cloud". By analysing the performance and security shows that proposed scheme is highly efficient and highly secure for time sensitive data in public cloud.

KEYWORDS: Cloud Storage, Data security, Fine-grained Access control, Timed-release encryption, CP-CBE (Ciphertext Policy Attribute Based Encryption).

I. INTRODUCTION

Cloud computing is a type of computing that relies on shared computing resources rather than having local servers or personal devices to handle applications. In its most simple description, cloud computing is taking services ("cloud services") and moving them outside an organization's firewall. Applications, storage and other services are accessed via the Web. The services are delivered and used over the Internet and are paid for by the cloud customer on an as-needed or pay-per-use business model. Cloud storage acts as an important service of cloud computing. It makes a way for the owners to update their data in the storage cloud which can be accessed by the end users anytime, anywhere across the world just by using the keys to decrypt the data. But since this is not a trusted service we make use of the ABE (Attribute Based Encryption) method for decryption which provides fine grained access control and also to protect the confidentiality of sensitive data. ABE is known for two forms:

1. KP-ABE (Key Policy Attribute Based Encryption)
2. CP-ABE (Ciphertext Policy Attribute Based Encryption)

In this project, we use the CP-ABE method for encryption and decryption of time sensitive data. CP-ABE provides a scalable way for encrypting the data in which owners specifies time and attributes while encrypting the data and those

attribute must be satisfied by the user to decrypt the data which helps in high data security. This project is implemented by combining both the time and attribute factors by embedding the timed-release encryption into CP-ABE for time-sensitive data in public cloud. We also make use of trapdoor mechanism which is an important feature of Timed-release encryption. The trapdoor mechanism used is related only to the time factor which makes our scheme highly efficient and feasible.

II. RELATED WORK

The work in [1] has few plans utilizing attribute based encryption (ABE) have been proposed to get control of outsourced information in distributed computing; A large portion of them experience the effects of rigidity in executing complex access control approaches. Keeping in mind the end goal to acknowledge versatile, adaptable, and fine-grained to get control of outsourced information in distributed computing. In this paper, various leveled attribute set-based encryption (HASBE) by expanding ciphertext-strategy attribute set-based encryption (ASBE) with a various leveled structure of clients. This plan not just accomplishes versatility because of its progressive structure, yet in addition acquires adaptability and fine-grained get to control in supporting compound properties of ASBE. Likewise, HASBE utilizes numerous esteem assignments for less lapse time to manage client denial more proficiently than existing plans. This paper formally demonstrate the security of HASBE in place of security of the ciphertext policy attribute based encryption (CP-ABE) conspire by Bethencourt et al. furthermore, examine its execution and computational multifaceted nature. It analyse the plan and demonstrate that it is both productive and adaptable in managing access control for outsourced information in distributed computing with thorough examinations.

The work in [2] discussed about Ciphertext Attribute based Encryption (CP-ABE) which is a promising procedure to get control of scrambled information. It requires a trusted specialist who deals with every one of the properties and circulates in the framework. In cloud storage frameworks, there are numerous specialists exist together and every specialist can issue properties independently. Notwithstanding, existing CP-ABE plans can't be specifically connected to information to get control for multi-expert distributed storage frameworks, because of the wastefulness of unscrambling and renouncement. In this paper, DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), a powerful and secure information to get control conspire with productive unscrambling and renouncement. In particular, it develops another multi-specialist CP-ABE conspire with effective unscrambling and furthermore outline a productive quality denial strategy that can accomplish both forward security and in reverse security. The investigation and the reproduction comes about to show that DAC-MACS is exceedingly effective and provably secure under the security display.

The work in [3] has few procedures, which have been explored, including encryption, and additionally fine-grained to get control for empowering such administrations. In any case, these systems just communicate the "Yes or No" issue, that is, regardless of whether the client has authorizations to get to the comparing information. This paper researches the issue of how to give distinctive granular data sees for various clients. The component first builds the connection between the catchphrases and information records in light of a Galois association. In addition, later it abuse information recovery lists with variable limit, where granular information recovery administration can be upheld by changing the edge for various clients. In addition, to anticipate security exposure, this proposes a differentially protection discharge plot in view of the proposed record method. This demonstrate the protection saving assurance of the proposed component, and the broad tests further show the legitimacy of the proposed component.

The work in [4] includes Open key coordinated discharge accessible encryption (PKTRSE) which can be utilized to tackle the time-subordinate ciphertext recovery issue. In coordinated PKTRSE, the sender transmits the scrambled message to the server and needs it to be viewed, also decoded by the special designated client after the discharge time. At the point when such PKTRSE is connected to scramble a message for various clients with a similar discharge time, its ciphertext estimate relies upon the client scale. To accomplish PKTRSE with steady expenses from the encryptor's and decryptor's point of view by acquiring the system of character based wide cast encryption. This proposes a cryptosystem of one to numerous PKTRSE which is called multi-client PKTRSE (MUPKTRSE). In MUPKTRSE, the sender transmits a scrambled message with the goal that the approved client gathering part can look through the objective ciphertext containing determined catchphrases before a pre-set discharge time, however each

approved client can't decode it until the point of the discharge time. This paper starts by clarifying what is MUPKTRSE and presenting the application situation of MUPKTRSE. At that point, It formalize the thought of MUPKTRSE and its security diversion.

The work in [5] has an thought called auditable σ - time outsourced CP-ABE, which is accepted to be relevant to distributed computing. As a sophisticated mechanism for secure fine-grained access control over encrypted data, ciphertext-policy attribute-based encryption (CP-ABE) is one of the highly promising candidates for cloud computing applications. However, there exist two main long-lasting open problems of CP-ABE that may limit its wide deployment in commercial applications. One is that decryption yields expensive pairing cost which often grows with the increase of access policy size. The other is that one is granted access privilege for unlimited times as long as his attribute set satisfies the access policy of a given ciphertext. Such powerful access rights, which are provided by CP-ABE, may be undesirable in real-world applications (e.g., pay-as-youuse). To address the above drawbacks, in this paper, it propose a new notion called auditable σ -time outsourced CP-ABE, which is believed to be applicable to cloud computing. In this notion, expensive pairing operation incurred by decryption is offloaded to cloud and meanwhile, the correctness of the operation can be audited efficiently. Moreover, the notion provides σ -time fine-grained access control. The cloud service provider may limit a particular set of users to enjoy access privilege for at most σ times within a specified period. As of independent interest, the notion also captures key-leakage resistance. The leakage of a user's decryption key does not help a malicious third party in decrypting the ciphertexts belonging to the user. This designs a concrete construction (satisfying our notion) in the key encapsulation mechanism setting based on Rouselakis and prime order CP-ABE, and further present security and extensive experimental analysis to highlight the scalability and efficiency of the construction.

III. SYSTEM DESIGN

Our scheme has an efficient architectural design in which an entity (The Central Authority CA) is responsible for timed-release function is redesigned. Apart from distributing the attribute-associated private keys CA also needs to provide access privileges, which is achieved by publishing the time-related tokens periodically. Since this architecture requires only a small amount of cost to provide the needed access control, it is reasonable and worthy. The additional overhead is also light weight in our design since there is no need for a secure channel between the CA and the data owners for the function of timed-release.

The system consists of four modules: CA (a central authority), Owner (several data owners), Users (many data consumers), Cloud (cloud service provider).

- **Cloud (Cloud service provider)** - It is nothing but the administrator of the cloud and cloud servers. Cloud is responsible to store a set of data from the data owners, accepts the user request and also helps the data owners and users to perform difficult computations.
- **CA (The central authority)** – The whole system's security protection is managed by the CA. It is responsible to distribute the private keys for each users based on the related attributes specified and also responsible to publish the parameters of the system. In addition to this, CA also acts as a time agent to publish the time related secret on each pre-defined time. □
- **Owner (The data owner)** – It is responsible for making decisions on access policy based on the attributes and release time, and then encrypts his data based on the decided policy before uploading it.
- **User (The data consumer)** – CA is responsible to provide the private keys for the users to decrypt the data. He/She can request any ciphertext data which is stored in the cloud but can decrypt it only if he/she satisfies both of the following constraints:
 - 1) His/her set of attributes must be satisfied for the access policy.
 - 2) The current time for accessing is later than the corresponding time for releasing the data.

DATA FLOW DIAGRAM

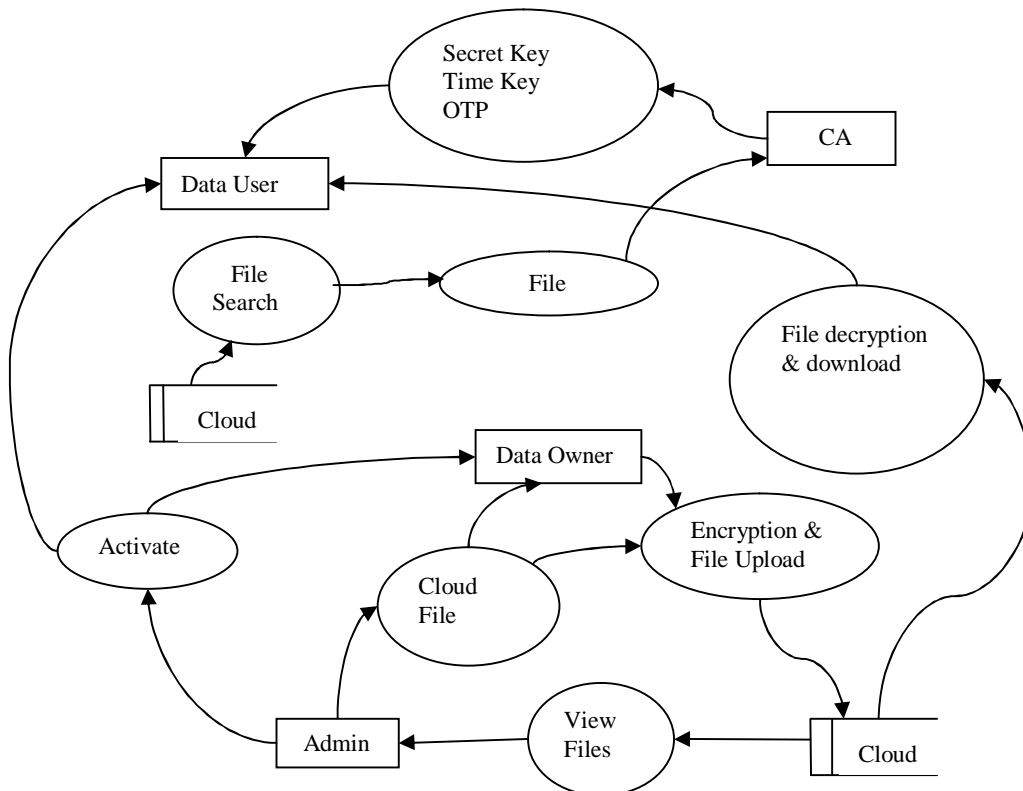


Fig.1: Dataflow Diagram Level

III. EXPERIMENTAL RESULTS

Figure shows the step by step procedure that each entity should follow while involved in fine grained data sharing on time sensitive data in public cloud. The entities involved here are data owner, Admin, data user from the below pictures we get the idea of home page of data Owner, data user, admin.

Figure (a) shows the home page of TAFC which consist of entities such as Admin, Data Owner Data User, CA. we can login to any of entity and check its current status.

Figure (b) shows Admin login page, where admin can directly login entering his admin id and password and then he can sign in to admin home page.

Figure (c) shows Admin home page, where admin can view uploaded files of data owner Data user request files, all uploaded files to cloud, time sensitive files, storage information and a logout option available.

Figure (d) shows the data user and his details like email id, mobile number to the admin, When he clicks on data user on Admin home page.

Figure (e) shows the Data Owner register page, which tells that data owner before uploading files he has to register to cloud.

Figure (f) shows home page of Data Owner, where he can upload files, upload secret key, view uploaded files and logout option.

Figure (g) shows how data owner can upload his file to cloud.

Figure (h) shows how he can view the uploaded Files.

Figure (i) shows user home page where user can search for file.


Figure (j) gives user file search result. Figure (k) shows that user can specify open and close time for data access.

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization *Volume 7, Special Issue 6, May 2018*
2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"
13th-14th March 2018
Organized by


Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Figure (l) shows how admin gets user file request. he will verify the request and if it is valid, then Admin will issue secret key to Data User.


(a) Home Page



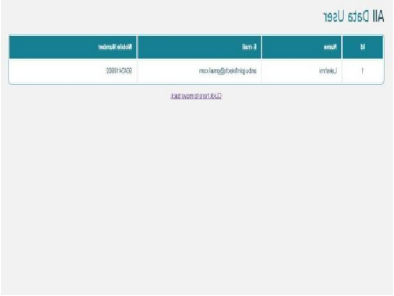
(b) Admin Login



(c) Admin Home Page

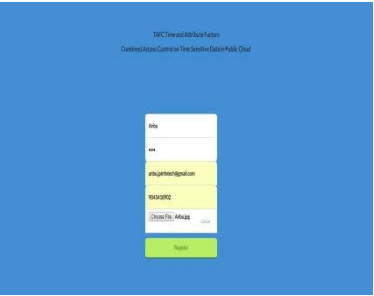


(d) View Data User




File ID	Data Owner Name	File Name	Request
1	Admin	Request	Request File


(e) Register




(f) Data Owner Home Page



(g) Upload File

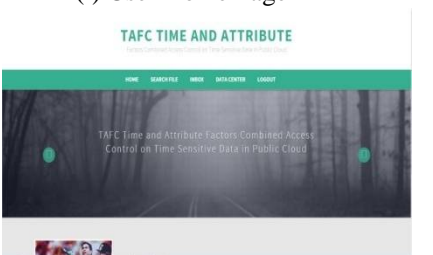


(h) View File

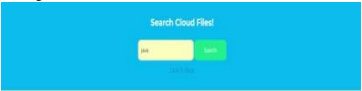


File ID	Data Owner Name	File Name	Request
1	Admin	Request	Request File

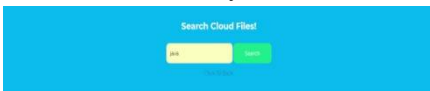
(i) User Home Page



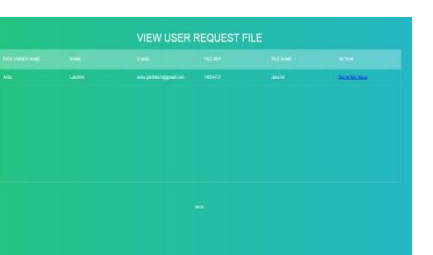
(j) User Search Result



(k) Time Key



(l) User Result



File ID	Data Owner Name	File Name	Request
1	Admin	Request	Request File

V.CONCLUSION

This paper aims for fine-grained access to get control for time touchy information in cloud storage. One test is to accomplish adaptable planned discharge and fine granularity with lightweight overhead, which isn't given in related work. In this paper, we propose a plan to accomplish this objective. Our plan consistently consolidates the idea of planned discharge encryption to the design of ciphertext Policy attribute based encryption. With a suit of proposed system, this plan furnishes data owner with the capacity to adaptably discharge the entrance benefit to various clients at various time, as per all around characterized to get arrangement over properties and discharge time. The analysis demonstrates that our plan can ensure the classification of time-touchy information, with a lightweight overhead on both CA and data owner, therefore well suits the practical extensive scale to get control framework 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] Z. Zhou, H. Zhang, Q. Zhang, Y. Xu, and 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.
- [4] 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.
- [5] Jianting Ning, Zhenfu Cao, Xiaolei Dong Kaitai Liang, Hui Ma, " Auditible σ -Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing", IEEE Transactions on information Forensics and Security vol. 13, no. 1, january 2018.
- [6] 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.
- [7] Hui Ma , Rui Zhang, Zhiguo Wan, Yao Lu, and Suqing Lin, "Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing", IEEE Transactions on Dependable and Secure Computing,vol.14, 14, no.6, November/December.