A Novel Technique for Cloud Computing Data Security and Public Auditing

Mr. Amir Ali
Department of Computer Science and Engineering
G.H Raisoni College of Engineering & Management
Wagholi, Pune

Prof. Nivedita Kadam
Department of Computer Science and Engineering
G.H Raisoni College of Engineering & Management
Wagholi, Pune

Abstract— In prior years, the fast improvement of cloud storage services makes it simpler than at any other time for cloud clients to disseminate information (data) with everyone. To ensure client's trust in the dependability of their public information on the cloud, various strategies have been proposed for information trustworthiness assessing with spotlights on different viable components, secure data destructing, public integrity auditing and so forth.. Since it is not achievable to execute full lifecycle protection security, access control turns into a testing assignment, particularly when we share delicate information on cloud servers. To handle this issue, proposed framework presents a key strategy trait based encryption with time-determined properties (KP-TSABE), another safe information self-destructing framework in distributed computing. Moreover open respectability inspecting frameworks presented for cloud information sharing administrations that check the uprightness of client's delicate information being put away in the cloud. In the KP-TABE plan, each figure content is marked with a period interim while the private key is connected with a period moment. The figure message just is unscrambled if both the time instant is in the permitted time interim and traits which are connected with the figure content guarantee the key's entrance structure. Also, Third Party Auditing (TPA) is acquainted with help clients to assess the danger of their subscribed cloud data administrations. The review result from TPA would likewise be useful for the cloud administration suppliers to upgrade cloud-based administration stage.

Keywords— *Sensitive data, assured deletion, fine-grained access control, privacy preserving, public auditing.*

*****

I. Introduction

Cloud computing imagined as the next generation information technology (IT) design for enterprises, because of its long list of new dedications within the IT history: location independent resource pooling, on-demand self-service, rapid resource elasticity, ubiquitous network access, usage-based evaluation and transference of risk. As a problematic innovation with attentive ramifications, distributed computing is changing the very way of however organizations use data innovation. One fundamental part of this outlook changing is that learning is being brought together or outsourced to the cloud. From clients' perspective, together with every person and IT endeavors, putting away information remotely to the cloud amid a multipurpose on-interest way brings fascinating advantages: alleviation of the Storage management, location independence, and dismissal of capital use on equipment (hardware), programming, and work force maintenance, and so on.

Distributed computing is considered as the following stride in the advancement of on-demand data innovation which consolidates an accumulation of existing and new strategies from examination territories like service-oriented architectures (SOA) and virtualization. With the quick development of adaptable cloud computing innovation and services, it is normal for clients to influence cloud storage services to impart information to others during a friend circle, e.g., Dropbox, Google Drive and AliCloud [1]. The mutual learning in cloud servers, in any case, commonly contains clients' delicate data (e.g., individual profile, budgetary information, health records, and so forth.) and wishes to be ensured [2]. as the responsibility for data is isolated from the administration of them [3], the cloud servers could relocate clients' learning to various cloud servers in outsourcing or share them in cloud seeking. [4]Consequently, it turns into a major challenge to ensure the protection of this shared knowledge in a cloud, especially in cross-cloud and huge information environment [5]. In order to fulfil this challenge, it's important to outline a complete determination to bolster client defined approval period and to give fine-grained access management all through this time. The shared information ought to act naturally destroyed when the client-defined lapse time. One of the methodologies to lighten the issues is to store data as a typical scrambled structure. The impediment of encoding information is that the client can't share his/her scrambled learning at a flawless level. When information proprietor requires sharing somebody his/her data, the proprietor ought to see precisely the one he/she needs to share with [6]. In a few applications, the information proprietor needs to share data to numerous clients in step with the security approach upheld the clients' credentials. Attribute-based encryption (ABE) has critical advantages supported the custom public key encryption instead of coordinated encryption as a consequence of it accomplishes adaptable one-to-many encryption. With the quick advancement of adaptable cloud services, heaps of most recent difficulties have developed. One amongst the chief imperative issues is an approach to safely erase the outsourced data put away on the cloud servers.

For the right execution of constant illustrations of Dropbox applications, one downside is to guarantee data respectability, i.e., each data alteration operation is so performed by an approved gathering part and, along these lines, the data stays in place and overhaul to date from that point. This drawback is vital given the real truth that cloud storage platforms, even surely understood cloud stages, could encounter equipment/programming failures, human mix-ups and outside malevolent assaults. to totally make sure the information integrity and save the cloud users' computation resources also the as on-line burden, it is of necessary importance to enable public auditing service for cloud information storage, so users could resort to an independent third-party auditor (TPA) to audit the outsourced information once required. The TPA has skills and abilities that clients don't, will occasionally check the integrity of all the data stored inside of the cloud on behalf of the clients that gives technique extra simpler and moderate path for the clients to affirm their capacity precision inside of the cloud. In addition, moreover to help clients to assess risk of their subscribed cloud data benefits, the review result from TPA would likewise be useful for the cloud service providers to improve their cloud-based service platform, and even fill for free mediation needs. In a word, empowering public auditing services can assume a key part in this early cloud economy to wind up completely settled; wherever clients can require routes that to survey hazard and pick up trust inside of the cloud.

The remainder of this paper is prearranged as: Section II briefly discusses the certain related effort. Section III describes the existing system with its limitations. In section IV, proposed system is explained with a system design and, in Section V, the system setup in the form of the mathematical equation is described. Lastly, in Section VI expected results are defined and in Section VII conclusion is summarized.

II. Literature Survey

In the literature review the topical methods over secure data retrieval are going to discuss.

TABLE I. LITERATURE DESCRIPTION

Ref No.	Authors	Proposed System	Drawback/future work
[1]	Boyang Wang et al. [2014]	Author proposed the privacy-preserving mechanism that allows public auditing on shared data stored in the cloud. Additionally exploited ring signatures to calculate the verification information required to audit the integrity of shared data.	A fascinating issue in their future work is the manner by which to productively review the respectability of shared information through element bunches though as yet saving the uniqueness of the signer on every square from the third Party auditor..
[10]	P. Tysowski and M. Hasan et al. [2013]	This paper presented a model for key distribution based on the principle of dynamic data re-encryption	The primary disadvantage with this methodology is the re-encryption errand required at whatever point bunch participation changes, which is a moderately costly operation..
[16]	Lingfang Zeng et al. [2013]	In this paper, authors projected SeDas, a mechanism that meets data privacy challenge through a new incorporation of cryptographic methods with active storage techniques supported T10 OSD standard.	This paper does not present object-based storage system designs for Cloud services.
[17]	Jinbo Xiong et al. [2013]	In this paper, authors propose an ABE-based secure document self-destruction (ADS) scheme, which is a new incorporation of attribute-based encryption (ABE) algorithm with global-scale, decentralized distributed hash table (DHT) network.	A significant direction of their future work is to design the different data lifetime to satisfy the diversity requirements of document privacy and security in cloud computing.
[5]	Pooyan Jamshidi et al. [2014]	This paper aims to identify, taxonomically classify and systematically compare existing research on cloud migration.	This paper focuses only on reviews of previous work.
[11]	Joel Reardon et al. [2013]	Authors have explored secure deletion. They defined the simple issue of removing data objects from physical medium and showed this problem has many complexities and nuances.	They hope that future task in secure data deletion takes advantage of this systematization by also dividing access to the physical medium into layers as well as implementing secure data deletion at the appropriate interface and level of abstraction.

III. Existing System

A. Existing System

The existing system model is defined by dividing the KP-TSABE scheme into the following six entities.

- Data owner. Data proprietor can convey data or documents that contain some delicate data, which is utilized for offering to his/her companions (data clients). This common information are outsourced to store on cloud storage servers.
- Authority. It is a vital article which is subject to making, issuing and dealing with all the private keys and also is trusted by the various elements included in the framework.
- Time server. It is a time reference server without any interaction with other entities involved in the system. It is responsible for an accurate release time specification.
- Data users. Data users are some people who passed the identity confirmation and access to the data outsourced by the data owner. Notice that the shared data can be accessed by only the authorized users during its permission period.
- Cloud servers. It contains almost limitless storage space which is able to store and manage all the data or files in the system. Other entities with limited storage space can store their data on the cloud servers.
- Potential adversary. It is a polynomial time adversary and described in the safety model of the KPTSABE scheme.

To form a basis for the KP-TSABE scheme following concepts are introduced:

- Authorization period. It is a time interval predefined by a data owner, starting from the desired release time and ending at the expiration time. The ciphertext is associated with this interval; the user can construct the decryption key only when the time instant is within this intermission.
- Expiration time. It is a threshold time instant predefined by the owner. The mutual data can only be accessed by the user before this time instant because the mutual data will be self-destructed after expiration.
- Full lifecycle. It is a time interval from the generation of the shared user's data, approval period to the expiration time. This paper delivers full lifecycle privacy protection for shared data in cloud computing.

B. Limitation of existing System

Limitations of existing system are illustrated as:

- Existing system does not handle data security checking process. User uploads data but not have authority to check integrity of that data.
- Existing system does not introduce any entity like Third Party (TPA).

IV. Proposed Architecture

A. Proposed System declares a Third Party inspector (TPA) to review client record demand for checking the honesty of the relating document. The third party auditor can publicly confirm the honesty of shared records or information for a gathering of clients without recovering the entire information. The TPA concerns a review lively content or test to the cloud server to guarantee that the cloud server has held the information appropriately at the time of the review or audit.

B. Architecture Overview

As in figure 1, the entities can explain as follows.
The Proposed system model is defined by dividing the KP-TSABE scheme into the following seven entities.

- **Data owner:** Data owner can provide data or files that contain some sensitive information, which is used for sharing with his/her friends (data users). All these shared data are outsourced to the cloud servers to store.
- **Authority:** It is an essential entity which is responsible for generating, distributing and managing all the private keys, and is confidential by all the other entities involved in the system.
- **Time server:** It is a time reference server without single interaction with other entities involved in the system. It is answerable for a precise release time specification.
- **Data users:** Data users are some people who passed the identity confirmation and access to the data outsourced by the data owner. Note that the user's shared data can be accessed by only the authorized users during its authorization period.
- **Cloud servers:** It contains almost unlimited storage space which is able to store and manage all the data or files in the system. Other entities with limited space for storage can store their data on the cloud servers.
- **Potential adversary:** It is a polynomial time adversary and described in the security model of the KPTSABE scheme.
- **TPA:** The Third Party Auditor (TPA) is an entity that able to publicly verify the integrity of shared information or file for a group of users devoid of retrieving the whole data. The TPA concerns an audit chipertext or challenge to the cloud server to ensure that the cloud server has reserved the data properly at the time of the audit.

C. Proposed Architecture Diagram

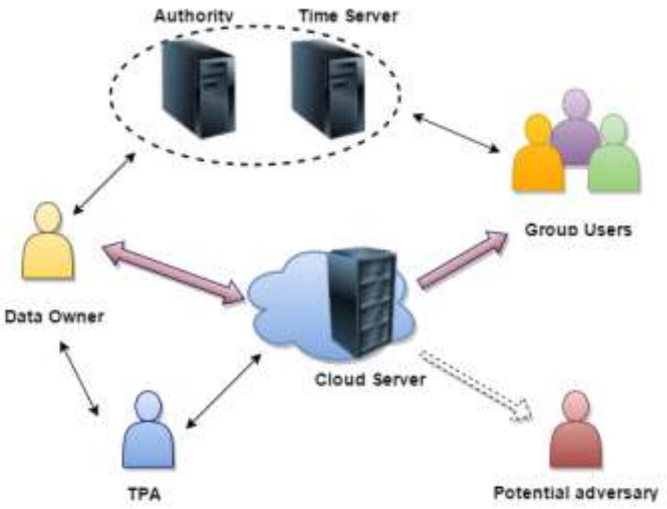


Fig. 1. Proposed Architecture

V. Proposed System Setup

The algorithm level of the KP-TSABE scheme includes four algorithms: Setup, Encrypt, KeyGen, and Decrypt.

1. Setup Phase:

Let T be the maximum time in the system provided by the time server which satisfies $|T|=n'$. Choose a security parameter k, and define the universe of all attributes
At= {1, . . . , n} [1].
The public parameters are distributed as:

$$params = \{g, g_1, g_2, \{\forall i = 1 : n, u'_{i,1}, u'_{i,2}\}, \{\forall j = 1 : T, u_j\}\}.$$

2. Encrypt:

To encrypt a message M under a set of attributes Satt with each attribute $i \in S_{att}$, where i is constrained by a time interval $T'_i \in [t_{m_{L,i}}, t_{m_{R,i}}]$, choose a random value $s \in \mathbb{Z}_p$, define $c_{L,i}$ as index, let $c_{L,i} = n' - m_{L,i}$ and publish the ciphertext as

$$CT = \left\{ C_M = M \cdot e(g, g_2)^{s\alpha}, g^s, \{S_{att}, \left\{ E = \left(u'_{i,1} \prod_{j=1}^{m_{R,i}+1} u_j^{t_j} \right)^s, E' = \left(u'_{i,2} \prod_{j=1}^{c_{L,i}} u_j^{T-t_j} \right)^s, T'_i \right\}_{i \in S_{att}} \right\}.$$

3. KeyGen:

This algorithm inputs the public parameters params, the master key MSK, the access tree Tr and the time instant set Tk. The algorithm proceeds as follows

Step1: First, it chooses a polynomial qx for each node x except the leaf nodes in Tr. Select root node r.

Step2: For non-leaf node x in Tr, set the degree dx of the polynomial qx and its threshold value kx satisfying qx=kx-1.

Step3: For the root node r, set qr(0)=y and choose other dr points randomly to completely define the polynomial qr.

Step4: For any other node x, set $q_x(0) = q_{parent(x)}(index(x))$ and pick dx other points of qx randomly to define it completely.

Step5: The algorithm randomly chooses $r_x, r'_x \in \mathbb{Z}_p$, defines nx be the index which lets $c_x = n' - n_x$, computes and gives the following secret value d to the user:

$$d = \{D_{x,1}, D_{x,2}, g^{r_x}, g^{r'_x}, u_{n_x+2}^{r_x} \cdots, u_T^{r_x}, u_{c_x+1}^{r'_x} \cdots, u_T^{r'_x}, t_{n_x}\}_{x \in S_Y},$$

Where,

$$D_{x,1} = g_2^{q_x(0)+r_x} \left(u'_{i,1} \prod_{j=1}^{n_x+1} u_j^{t_j} \right)^{r_x},$$
$$D_{x,2} = g_2^{-r_x} \left(u'_{i,2} \prod_{j=1}^{c_x} u_j^{T-t_j} \right)^{r'_x}.$$

4. Decrypt:

The decryption procedure is a recursive algorithm which is from bottom to up. In order to decrypt the ciphertext successfully, the valid attribute set should satisfy Tr. For the leaf node x: If $t_{n_x} \notin [t_{m_{L,x}}, t_{m_{R,x}}]$ the decryption algorithm simply outputs ?. Otherwise, the algorithm chooses random $r''_x, r'''_x \in \mathbb{Z}_p$ and calculates

$$d_{upp1} = \{a_0, g^{r_{R,x}} \cdot g^{r''_x}, u_{m_{R,x}+2}^{r_{R,x}} \cdot u_{m_{R,x}+2}^{r''_x} \cdots, u_T^{r_{R,x}} \cdot u_T^{r''_x}\},$$

$$d_{upp2} = \{b_0, g^{r_{L,x}} \cdot g^{r'''_x}, u_{c_{L,x}+1}^{r_{L,x}} \cdot u_{c_{L,x}+1}^{r'''_x} \cdots, u_T^{r_{L,x}} \cdot u_T^{r'''_x}\},$$

Where,

$$a_0 = D_{x,1} \left(u'_{i,1} \prod_{j=n_x+1}^{m_{R,x}+1} u_j^{t_j} \right)^{r_{R,x}} \left(u'_{i,1} \prod_{j=1}^{m_{R,x}+1} u_j^{t_j} \right)^{r''_x}$$
$$= g_2^{q_x(0)+r_x} \left(u'_{i,1} \prod_{j=1}^{m_{R,x}+1} u_j^{t_j} \right)^{r_{R,x}+r''_x}.$$

$$b_0 = D_{x,2} \left(u'_{i,2} \prod_{j=c_x}^{c_{L,x}} u_j^{T-t_j} \right)^{r_{L,x}} \left(u'_{i,2} \prod_{j=1}^{c_{L,x}} u_j^{T-t_j} \right)^{r'''_x}$$
$$= g_2^{-r_x} \left(u'_{i,2} \prod_{j=1}^{c_{L,x}} u_j^{T-t_j} \right)^{r_{L,x}+r'''_x}.$$

Then, the algorithm calculates as follows:

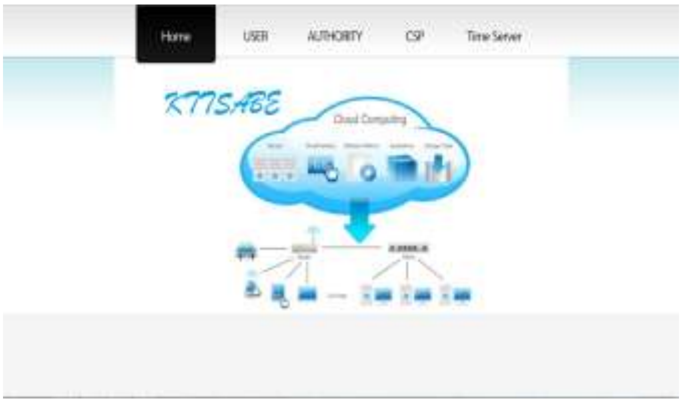
$$DN = \frac{e(g^s, a_0) \cdot e(b_0, g^s)}{e(E, g^{r_{R,x}+r''_x}) \cdot e(g^{r_{L,x}+r'''_x}, E')} = e(g, g_2)^{sq_x(0)}$$

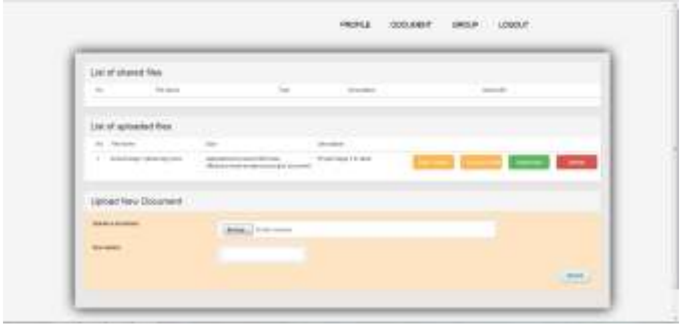
VI. Results

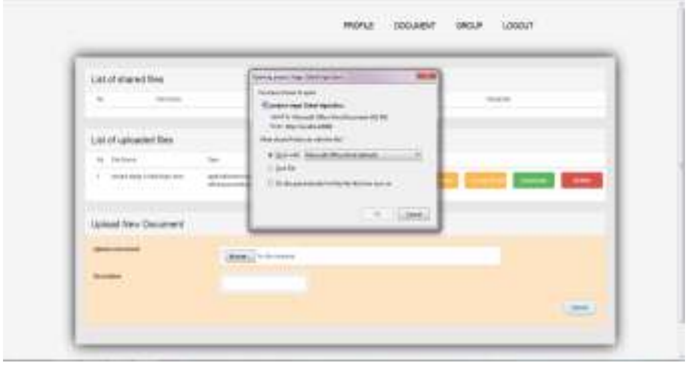
Some outcomes are resulting from this scheme:

Confidentiality: Confidentiality refers to just authorized parties or systems having the ability to access protected information of the user.

Integrity Auditing: Data Integrity refers to the defence of user information from illegal deletion, updating our construction stored in the cloud.







VII. Conclusion

This report exhibited a proposed KP-TSABE plan which can accomplish the time specified ciphertext keeping in mind the end goal to take care of these issues by actualizing adaptable fine-grained access control during the authorization period and time-controllable self-destruction after lapse to the shared and outsourced data in cloud computing. We additionally gave a system model and a security model for the KP-TSABE plan. Also, this paper plans a privacy-preserving public auditing approach for data storage security in cloud computing utilizing TPA. The TPA would not realize any information about the data content stored on the cloud server all through the effective auditing system, which not just rejects the weight of cloud client from the repetitive and perhaps costly reviewing assignment additionally enhances the clients' apprehension of their outsourced data surge.

References

[1] J. Xiong, X. Liu, Z. Yao, J. Ma, Qi Li, K. Geng, and P. S. Chen, A Secure Data Self-Destructing Scheme in Cloud Computing, IEEEtrans on cloud computing, vol. 2, no. 4, oct-dec 2014.

[2] B. Wang, B. Li, and H. Li, “Oruta: Privacy-preserving public auditing for shared data in the cloud,” IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43–56, Jan.–Mar. 2014.

[3] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, “Priam: Privacy preserving identity and access management scheme in cloud,” KSII Trans. Internet Inf. Syst., vol. 8, no. 1, pp. 282–304, 2014.

[4] J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, “A full lifecycle privacy protection scheme for sensitive data in cloud computing,” Peer-to-Peer Netw. Appl., Jun. 2014, DOI:10.1007/ s12083-014-0295-x.

[5] P. Jamshidi, A. Ahmad, and C. Pahl, “Cloud migration research: A systematic review,” IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 142–157, Jul.–Dec. 2013.

[6] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, “Toward efficient and privacy-preserving computing in big data era,” IEEE Netw., vol. 28, no. 4, pp. 46–50, Jul./Aug. 2014.

[7] X. Liu, J. Ma, J. Xiong, and G. Liu, “Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data,” Int. J. Netw. Security, vol. 16, no. 4, pp. 351–357, 2014.

[8] K. G. Paterson and E. A. Quaglia, “Time-specific encryption,” in Proc. 7th Int. Conf. Security Cryptography Netw., 2010, pp. 1–16.

[9] Q. Li, J. Ma, R. Li, J. Xiong, and X. Liu, “Large universe decentralized key-policy attribute-based encryption,” Security Commun. Netw., Mar. 2014, DOI: 10.1002/sec.997.

[10] P. Tysowski and M. Hasan, “Hybrid attribute- and re-encryptionbased key management for secure and scalable mobile applications in clouds,” IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172– 186, Jul. 2013.

[11] J. Reardon, D. Basin, and S. Capkun, “Sok: Secure data deletion,” in Proc. 34th IEEE Symp. Security Privacy, 2013, pp. 1–15.

[12] C. Cachin, K. Haralambiev, H.-C. Hsiao, and A. Sorniotti, “Policybased secure deletion,” in Proc. ACM Conf. Comput. Commun Security, 2013, pp. 152–167.

[13] J. Reardon, H. Ritzdorf, D. Basin, and S. Capkun, “Secure data deletion from persistent media,” in Proc. ACM Conf. Comput. Commun Security, 2013, pp. 271–284.

[14] J. Xiong, Z. Yao, J. Ma, F. Li, and X. Liu, “A secure self-destruction scheme with IBE for the internet content privacy,” Chinese J. Comput., vol. 37, no. 1, pp. 139–150, 2014.

[15] G. Wang, F. Yue, and Q. Liu, “A secure self-destructing scheme for electronic data,” J. Comput. Syst. Sci., vol. 79, no. 2, pp. 279–290, 2013.

[16] L. Zeng, S. Chen, Q. Wei, and D. Feng, “Sedas: A self-destructing data system based on active storage framework,” IEEE Trans. Magnetics, vol. 49, no. 6, pp. 2548–2554, Jun. 2013.

[17] J. Xiong, Z. Yao, J. Ma, X. Liu, and Q. Li, “A secure document selfdestruction scheme: An abe approach,” in Proc. 15th IEEE Int. Conf. High Perform. Comput. Commun., 2013, pp. 59–64.

[18] J. Xiong, Z. Yao, J. Ma, F. Li, X. Liu, and Q. Li, “A secure selfdestruction scheme for composite documents with attribute based encryption,” Acta Electronica Sinica, vol. 42, no. 2, pp. 366–376, 2014