International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

A SECURE SELF-DELETION METHOD FOR DATA ON CLOUD STORAGE

Prof. Anil Kumar Warad[1], Ayesha Shikalgar[2], Arti Kumari[3] Pranali Talghade[4]

[1]*Assistant Professor, P.G.M.C.O.E, Wagholi*
[2] *Student, Dept. of Computer Engineering, P.G.M.C.O.E college, Pune,India*
[3]*Student, Dept. of Computer Engineering, P.G.M.C.O.E college, Pune,India*
[4] *Student, Dept. of Computer Engineering, P.G.M.C.O.E college, Pune,India*

Abstract – *Cloud computing is the next generation in the field of on-demand information technology. This is a combination of the already existing and the newly emerging techniques from virtualization and service oriented architecture like research areas. Cloud storage removes the burden of locally storing and maintaining of data or application in spite of so many advantages of cloud computing, in case of sensitive data on cloud servers, access control is a major challenge. For this problem to be overcome, here we give a detailed study of certain previous and recent methods. This study ranges from encryption of data before storing to the recent method key attributes-based encryption with time specified attributes (KABE-TSA). The KABE-TSA is a self-deleting scheme in cloud computing.*

The KABE-TSA is in a place to resolve some necessary security problems by supporting user outlined authorization quantity and by providing fine-grained access management all through the quantity, the sensitive info are aiming to be firmly self-destructed once a user-specified expiration time, the KABE-TSA theme is tried to be secure beneath the choice l-bilinear Diffie-Hellman inversion (l-Expanded BDHI) presumption, comprehensive distinction of the protection properties indicate that the KABE-TSA theme planned by USA satisfies the protection wants and is superior to alternative existing schemes.

Key Words: **Self-Deleting, KABE-TSA, Fine Grained Access, Privacy-Preserving, Sensitive information, , Privacy-protection, Cloud Computing**.

1. INTRODUCTION

The shared information in cloud servers, however, usual contains users' sensitive knowledge (e.g., personal profile, financial information, health records, etc.) and inclination to be protected [1], as a result of the possession of the info is allotted from the supply of them [3], the cloud servers might migrate users' information to different cloud servers in outsourcing or unfold them in cloud looking [4], therefore, it becomes a vast challenge to safeguard the privacy of those shared details in cloud, notably in cross-cloud and large information atmosphere [1], thus on satisfy this challenge, it's necessary to vogue a comprehensive resolution in reality user-defined authorization quantity and to produce fine-grained access management throughout this era, the distributed information thought to be self-destroyed once the user-defined expiration time.

One of the ways that to alleviate the issues is to store information as a typical encrypted kind, the disadvantage of encrypting info is that the user cannot share his/her encrypted information at a fine-grained level, once a information owner needs to share somebody his/her data, the owner got to apprehend specifically the one he/she needs to share inside many applications, information owner needs to share information with many users in line with the safety policy supported the users' credentials, attribute based totally secret writing (ABE) has vital edges supported the tradition public key secret writing instead of matched secret writing as a results of it achieves versatile one-to-many secret writing ABE theme provides a powerful ability to realize each information security and fine-grained access management within the key-policy ABE (KABE) theme to be convoluted throughout this paper, the cipher text is labeled with set of descriptive attributes exclusively the set of descriptive attributes satisfies the access structure within the key, the user will get the plain text.

In general, the owner has the correct to specify that sure sensitive knowledge is simply valid for a restricted quantity of it slow, or mustn't be free before a particular time, timed-release secret writing (TRE) provides a remarkable secret writing service wherever associate in nursing secret writing secret's related to a predefined unharnessed time, and a receiver will entirely construct the corresponding secret writing key throughout currently instance, on this basis, Paterson et al, projected a time specific secret writing (TSE) theme, that's in an exceedingly position to specify Associate in Nursing acceptable live given the cipher text will entirely be decrypted throughout this interval (decryption live, DTI). it ought to use in many applications, e.g., web programming contest, electronic sealed-bid auction, electronic sealed-bid auction are often a method to determine the worth of

merchandise through world wide net whereas keeping the bids secret throughout the bidding section, i.e, the bids (cipher text) ought to be compelled to be unbroken secret throughout the bidding section (a specific time interval).

However, applying the ABE to the shared information will introduce many issues with relevance time specific constraint and self-deleting, whereas applying the TSE can introduce issues with relevance fine-grained access management. Thus, throughout this paper, we've got an inclination to rearrange to unravel these issues by pattern KPABE and adding a constraint of someday interval to every attribute within the set of secret writing attributes.

In CPABE, the cipher text is said to the gain structure whereas the private key contains a set of attributes, Bethen court et al. projected the first CPABE theme, the disadvantage of their theme is that security proof was entirely created below the generic cluster model to alter this weakness, Cheung et al. presented another construction below a typical model, set of access structures over the properties and projected a cost-effective associated demonstrably secure CP-ABE theme below the standard model [7].

In KP-ABE, the construct is reversed the cipher text contains a set of attributes and additionally the non-public secret is said to the access structure the first construction of KP-ABE theme was projected, in their theme, once a user created a secret request, the trusty authority determined that combination of attributes ought to appear inside the cipher text for the user to decipher. instead of victimization the Shamir secret key technique inside the non-public key, this theme used a lot of generalized sort of secret sharing to impose a identity access tree, Ostrovsky et al. introduce the primary KP-ABE system that supports the likelihood formulas in key policies Yu et al. used a fusing technique of KP-ABE, proxy re-encryption and lazy re-encryption that allows knowledge owner to delegate most of the computation tasks involved in fine-grained information access management to dubious cloud servers whereas not revealing the first data contents, Tysowski et al. changed the ABE and leveraged re-encryption algorithm to propose a totally distinctive theme to safeguard mobile user's data in cloud computing atmosphere.

Due to the shortage of some time constraints, the preceding ABE schemes do not support user-defined authorization amount and secure self-deleting once expiration for privacy-preserving of the data life cycle in cloud computing

1.1. Goals and Objectives

To developed the self deleting and location changing of file which is uploaded by user incase of making this document more secure that no one can hack it or theft it easily.

This system is developing so that only the intended recipient can use it by using the last notification which he is getting from the cloud account.

1.2. Motivation

During uploading/downloading of document we tend to aren't certain concerning its privacy and security as a result of it are often simply traced, hacked and thievery by others. Therefore to produce security and privacy from attackers this method of self deleting and site modification is to be implementing.

The state of art of secure self-deleting strategy, each SSDD and FullPP have some restriction, First, SSDD doesn't take into consideration the matter of the specified unharnessed time of the sensitive data, the expiration time of every SSDD and FullPP schemes is restricted by the DHT network and can't be determined by the user, second, it is consummate awful the vanish theme is liable to the Sybil attacks from the DHT network, the SSDD theme and various schemes square measure similar.

As consequences unauthorized users can freely access to the sensitive info and flaw would cause a major privacy human action. to assign with these disadvantage, we've got an inclination to propose a singular resolution call key policy attribute based totally secret writing with time specific attributes theme, in wise cloud application scenario, each info item is said to a specification of sometime interval decipherment quantity (DII), e.g. [1:00 to 8:00] denoting that the encrypted info item entirely be decrypted between 1:00 to 8:00 on specific info and it'll not be redeemable before 1:00 and once 7:00 that day.

If the time existent isn't among the precise quantity, the cipher text can't be decrypted, i.e., this cipher text square measure self destructed and no-one can decipher it. as a result of the expiration of the secure key. Therefore, secure info self-deleting with fine-grained access management is achieved.

2. LITERATURE REVIEW

Here the study of comparison of previous methods for security of data is presented. By these we come to know the demerits of the previously introduced techniques and the need for new data security techniques in cloud computing.

Goyal, O. Pandey, A. Sahai, Attribute-based encryption[1] ACM 2006:
ABE for fine grained access control of encryption data, here the introduction to key-policy ABE is being highlighted. In this a set of attributes are used to label the cipher text and to control which cipher text can be decrypted by which user association of private key with access structure is done.

New technique for fine grained access control are introduced. In this, as per the secure policy different users can decrypt the different pieces of data which is stored on servers in an encrypted format.

The set of attributes using which the data is encrypted are not hidden in this construction. Hiding set of attributes problem is left open in this.

Dr.P.K.Rai, Data Security and Privacy Protection Issues in Cloud Computing, PP 39-44 Feb. 2014:
Even though cloud computing has many potential benefits and many other activity applications still, when it comes to business captious applications especially in large enterprises do not prefer to move them to cloud.

Cloud computing is not conventionally being used market due to primary issues of security and privacy of data.

In this paper the summary but also over all analysis od data security and privacy protection issues related with cloud computing across all the stages of data life cycle is done

3. THE PROPOSED SCHEME

We propose a key-policy attribute-based secret writing with time-specified attributes (KABE-TSA), a unique secure information self-destructing theme in cloud computing within the KABE-TSA theme, each cipher text is labeled with a amount whereas non-public keys related to a time instant, the cipher text will solely be decrypted if each the time instant is within the allowed amount and also the attributes related to the cipher text satisfy the key's access structure.

The KABE-TSA is ready to resolve some vital security issues by supporting user outlined authorization amount and by providing fine-grained access management throughout the amount, the sensitive information is firmly self-destructed when a user-specified expiration time, the KABE-TSA theme is well-tried to be secure below the choice l-bilinear Diffie-Hellman inversion (l-Expanded BDHI) expectation, comprehensive differentiation of the safety properties indicate that the KABE-TSA theme projected by U.S. satisfies the safety needs and is superior to alternative existing schemes.

KABE-TSA doesn't want the majority efficacious assumption

3.1. Concepts and Models

3.1.1. Authorization:-

During this module, it's a interval predefined by a data owner starting from the desired unleash time and ending at the expiration time, the cipher text is propounded to the present interval, the user can construct the decoding key providing the time immediate is inside the interim.

3.1.2. Expiration :-

It's a threshold time instant predefined by the owner, the distributed data can only be retrieved by the user hitherto instant, as a results of the shared data area unit aiming to be self destructed once expiration.

3.1.3. Full Life Cycle:-

It's a interval from creation of the distributed data, authorization proportion to expiration time, this paper provides full life cycle privacy protection for shared data on cloud in cloud computing.

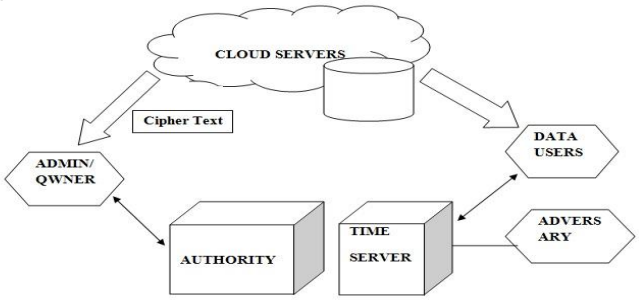

Figure 1. System model of KABE-TSA

To form a basis for the KP-ABTS theme, we have an inclination to tend to introduce the next ideas:

(1) *Admin / Owner* : Data owner will give information or files that contain some sensitive data, that ar used for sharing with his/her friends (data users). of these shared information ar outsourced to the cloud servers to store.

(2) *Authority* : It is an important entity that is to blame for generating, distributing and managing all the personal keys, and is trustworthy by all the opposite entities concerned within the system.

(3) *Time Server* : It is a time reference server with none interaction with different entities concerned within the system. it's chargeable for an exact unharness time specification.

(4) *Data Users* : Data users square measure some peoples WHO passed the identity authentication and access to the information outsourced by the information owner. Notice that, the shared knowledge will solely be accessed by the licensed users throughout its authorization amount.

(5) *Cloud Servers* :It contains virtually unlimited cupboard space that is ready to store and manage all the information or files within the system. different entities with restricted cupboard space will store their information to the cloud servers.

(6) *Adversary*. It is a polynomial time adversary.

4. COMPARISON AND ANALYSIS

The KABE-TSA theme is verified to be secure below the quality model. Therefore, we have a tendency to tend to tend to consistently compare this theme with this self destruction resolution (e.g., SSDD, and FullPP) from above aspects.

User defined authorization: Dematerialize, SSDD and FullPP leverage the DHT network to store the key shares or the hybrid cipher text shares, that area unit self discarded by the DHT nodes once a quantity of it slow that the expiration time is restricted by the update quantity of the DHT network and it can't be controlled by the sensitive knowledge owner however in KABE-TSA it's a lot of versatile to outlined by the user however the authorization amount and expiration time don't seem to be restricted by the system.

Attributes of security	**SSDD**	**FULLPP**	**KABE-TSA**
Supporting user-defined time intervals	NO	HALF	YES
Destructed cipher text or not?	YES	YES	NO NEED
Destructed key or not?	YES	YES	NO NEED
Fine-grained access support?	NO	YES	YES
Algorithms?	Symmetric	ID-TRE	KP-ABTS
Full life cycle protection (privacy) provided?	NO	YES	YES

Table 1: Comprehensive comparisons of the security properties

Prerequisite condition. All the schemes of Vanish [5], SSDD [6] and ISS [4] want the best assumption "no attacks on VDO before it expires". Since a Sybil mortal is ready to crawl enough key shares from the DHT network to reconstruct the decoding key. Once the mortal gets the VDO from the cloud servers before it expires, he/she can decode it with the reconstructed decoding key to get the plaintext. FullPP [3] doesn't want this ideal assumption as a result of the decoding secret's encrypted by the ID-TRE algorithmic rule. though the mortal crawls enough key shares from the DHTnetwork, he cannnot reconstruct the decoding key since he doesn't have the ID-TRE personal key. KABE-TSA additionally doesn't want the best assumption as a result of it doesn't need the DHT network.

5. CONCLUSION

With the quick/speedy development of versatile cloud services a lot of latest challenges have emerged. one altogether the foremost necessary issues is that the because of totally delete the expand data hold on within the cloud severs. throughout this paper, we've a bent to planned a unique KABE-TSA theme that is throughout a footing to grasp the time-specified cipher text so on unravel these issues by implementing versatile fine-grained access management throughout the authorization amount and time-controllable self-deleting once expiration to the shared and outsourced data in cloud computing, we've a bent to along provides a system model and a security model for the KABE-TSA theme, moreover, we've a bent to proof that KABE-TSA is secure at a lower place the quality model with the selection l-Expanded BDHI assumption. the nice analysis indicates that the planned KABE-TSA theme is superior to totally different existing schemes.

ACKNOWLEDGEMENT

We are very thankful to all the teachers who have provided us valuable guidance towards the completion of this project on A secure self-deletion method for data on cloud storage in cloud computing as part of the syllabus of bachelor's course. We express our sincere gratitude towards cooperative departments who has provided us with valuable assistance and requirements for the system development.

We are very grateful and want to express our thanks to head of department prof. Shrikant Dhamdhere sir for guidance in right manner, correcting our doubts by giving us their time whenever we required, and providing their knowledge and experience in making this project.

The acknowledge will be incomplete if we do not thank our dear Friends who helped us round the clock, which has been very helpful in building our project.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014.

[2] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme in cloud," KSII Transactions on Internet and Information Systems (TIIS), vol. 8, no. 1, pp. 282–304, 2014.

[3] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: A systematic review," Cloud Computing, IEEE Transactions on, vol. 1, no. 2, pp. 142–157, 2013.

[4] J. Xiong, Z. Yao, J. Ma, F. Li, and X. Liu, "A secure selfdestruction scheme with ibe for the internet content privacy," Chinese Journal of Computers, vol. 37, no. 1, pp. 139–150, 2014.

[5] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in Proceedings of the 18th USENIX Security Symposium, 2009, pp. 299–315.

[6] G. Wang, F. Yue, and Q. Liu, "A secure self-destructing scheme for electronic data," Journal of Computer and System Sciences, vol. 79, no. 2, pp. 279–290, 2013.

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