International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2015): 3.791

A Survey on Cloud Based Secure Self Destruction Accessibility with Time and Location

Akhil Shinde[1], Sayali Sant[2], Vedika Chavan[3], Ganesh Jagdale[4], Manjushri Mahajan[5]

[1, 2, 3, 4]Students, Dept. of CE, G. H. Raisoni College of Engineering and Manag- ement, Wagholi, Savitribai Phule University, Pune, India

[5]Assistant Professor, Dept. of CE, G. H. Raisoni College of Engineering and Management, Wagholi, Savitribai Phule Pune University, Pune, India

Abstract: ***Now a day, use of cloud is becoming easier to accessing data throughout the internet as well as easy to share file. During this lifecycle privacy security and also access control becomes challenging task especially when wants to share someone important data with anyother. This problem, can be solved using "key policy attribute based encryption with time based attribute (KP-TSABE)" and "location based attribute", a new secure data self destruction scheme on cloud computing. In this method every cipher text is labeled with specific time interval and also location of user who will access, in which private key is associated with time interval. This cipher-text can only be decrypted if and only if the time interval and location is matched. It also provides the security by using the authorization period and secure fine grained access control during that period. The files will be self-destructed if time interval expires. This proposed system can provide data security from the third party user.***

Keyword: cloud computing, privacy preserving, sensitive data, secure file grained access, secure self destruction

1. Introduction

Cloud computing is the next step into the digital world. We use cloud for storing data into the virtual storage space. Cloud based on distributed computing. Cloud is nothing but the collection of hardware and software. We can share our data with the other user. But cloud service provider provides security on the form of data encryption and decryption. In cloud computing three strategies are used,

1) Public Cloud
2) Private Cloud
3) Hybrid Cloud

Private cloud more secured than public. Our aim is increased use of public cloud. For that we focused on sharing data. Cloud service provider, e.g. Microsoft Azure, AWS(Amazon Web Services), Dropbox, Google Drive etc. is provide services as well as managing user profile, stored data, billing and so on. We want to prevent shared data from the third party user those haven't access permissions. For that we used "key policy attribute based encryption with time based attribute (KP-TSABE)" and "location based attribute".

2. Related Work

1) ORUTA: Privacy-preserving public auditing for shared data in the Cloud.

On the cloud, data stored on the entrusted cloud storage can be easily lost or corrupted due to hardware failures and some human errors. For this problem and to protect the integrity of data on cloud, it is best to use public auditing by introducing the third party auditor. Firstly, the provable data possession (PDP) mechanism is used to perform the public auditing to check the correctness of data stored on entrusted server, without retrieving the entire data. In the next step, Wang designed public auditing mechanism for data, so during public auditing the private data of the personal user is not displayed to the third party auditor. The most probable problem during the public auditing on cloud is how to preserve the identity privacy from the TPA (Third Party auditor). Because the identity of signer indicate the particular user in the group having higher valuable target than others.

In ORUTA, new system is defined for the privacy preserving public auditing mechanism on an entrusted cloud. In this system we develop the ring signatures to construct the homomorphic authenticators, so the third party auditor can easily verify the integrity of data for a group of users without retrieving the entire data. During this operation the identity of signer on each block is kept private from TPA. In addition, they develop mechanism to support batch auditing, in which we can audit multiple files simultaneously in a single auditing task.

In this paper, three parties are used: one is cloud server, second is third party auditor and third is users. And there are two types of users, the original user and number of group user. Both of this is member of the group. These group members are allowed to access and modify the shared data created by the original user based on access control policies. On the cloud, shared data and verification information is stored. To check the integrity of the shared data third party auditor is used.

This system is only developed for the static groups to check the integrity of the shared data in the cloud. That means the members of the group must be predefined in the group that cannot be changed during the data sharing. In this system, Interesting problem is that for the dynamic groups in which adding new user to the group, and removing the existing user from the group while still preserving identity privacy [1].

2) PRIAM: Privacy preserving identity and access management scheme in cloud

On the cloud, there are huge numbers of owners and users that can pay for the storage space on the cloud for limited period of time. Every owner and user has some specific identity. This identity information is stored on the cloud. For those owners and users it is necessary to construct privacy preserving identity management and access control mechanism for cloud computing. Cloud service providers (CSP) depend on owners and user's identity information to provide

appropriate access control so that cloud resources only accessed by the authorized users who are willing to pay. Owners and users wish to protect their personalized service access patterns, identity privacy information and accessing new cloud services by on demand ways within the scope of their permissions [2]. There are many identity authentication and access control schemes to address these challenges, however, there are still some limitations.

For this purpose they design new interesting technique, called Privacy preserving Identity and Access Management scheme, referred to as PRIAM, which have ability to satisfy all the desirable security requirements in cloud computing. In this system they use six types of users, named as users, cloud service providers(CSP), Registration server, Auditor server, Authentication and policy decision point(PDP) with back-end access control policy repository and cloud services policy enforcement point (PEP) respectively. The main contributions of the PRIAM scheme are three fold. First, it leverages blind signature and hash chain to protect user's identity privacy and implement secure mutual authentication. Second, it employs the service-level agreements to provide flexible and on-demand access control for both tenants and cloud services. Third, it makes use of the BAN logic to formally verify the correctness of the proposed protocols.

In this system, users can access the different authorized cloud services, it can access service with SID via nearby PEP. Registration server takes charge of registration of users and different cloud services. PEP receives service request from the users and forward it to PDP. After receiving a access grant from PDP, PEP allows users to access the required service within access permissions. PDP decides whether or not to authorize users based on the description of users attributes along with SLA. CSP provides authorized users and develops a cloud service. It needs to join the system and sends the join request to RS. AS is online third party server, which is used for collection of all sessions records, including registrations, access requests, access decisions, etc.

The main aim of PRIAM is to provide users privacy protection and authentication between Users and PDP. IT also provides on-demand access to cloud services for the users on cloud. It also provides the advantages like simplicity, correctness, low overhead and efficiency [2].

3) Cipher text-policy hierarchical attribute-based encryption for fine-grained access control of encryption data

In ciphertext policy hierarchical attribute based encryption (CP_HAB) Scheme, Data provider defines data is encrypted under the access structure, while private key is related with set of attributes. Characteristics of attributes are treated as same levels in most proposed system, while the attributes are always in different levels in real world circumstances. Generalization of tradition CP-ABE, the CP-HABE scheme is proved to be secure under the decisional q-parallel bilinear Diffie-Hellman exponent assumption. In CP-HABE scheme, attribute are assumed to be divided into m+1 level.

According to their importance in the system, different attribute belongs to different level. Set of attribute in hierarchy associate that every user hold the private key. In hierarchical access structure in the Ciphertext, when this attributes match, the user can get message from the sender. The CP-ABE uses the following algorithm i.e. Setup, Encrypt, Decrypt, Keygen. This scheme it is provides Fine grained access control and data security, and over the traditional ABE schemes according to practical situation this scheme exhibit significant improvement. Size of ciphertext is not constant, so how to improve CP-HABE scheme with a ciphertext of a constant size. How can we relocate attributes in different level more efficiently. How we can construct efficient scheme with attribute in hierarchy [3].

4) Time-specific encryption

Time specified encryption is new concept introduce in this paper. At the beginning of each time unit, a Time Instant Key (TIK), a time server broadcast a key in plain TSE. The message can specify any time interval by sender during the encryption process, the message can be decrypt by receiver only if it has TIK that corresponds to a time in that interval. The Time Specified encryption model introduces security model for plain, public key, and identity based setting.

In the communication time has always play the important role. After the certain point information become the useless, before a particular time sensitive data may not be released or may enabled access to information for only a limited period of time. The interesting property is in what time interval a ciphertext can be decrypted by a receiver.TSE time specified encryption, a new cryptographic primitive is introduce to have access to information for an unlimited period of time. It is available to all users in the form of TIK [4].

5) Secure Data Deletion from Persistent Media

The task of deleting data doesn't recoverable from a physical medium for secure data deletion. We present general approach of deletion for persistent storage that relies on encryption and key wrapping to the design and analysis and also introducing generic update function. It proves that it achieves secure deletion of data against a coercive attacker, instances of the update function implement the update behavior of all arborescent data structures. It including B-Trees, extendible hash tables, linked lists, and others. Some well-known technique like encryption technique to make data irrecoverable to unauthorized to access it. By coercive adversaries to long-term encryption keys are vulnerable to disclosure. User is unable to recover data when encrypted data is only securely deletion.

It is necessary to securely delete the key for securely delete data, a technique first used by Boneh and Lipton to securely delete data written onto magnetic tape for off-line archiving. A coercive attacker requires that the user who securely deletes data is there after unable to recover the deleted data against secure data deletion.

The user must ensure that the corresponding decryption key is securely deleted when the adversary already has an encrypted copy of the data being deleted. The decryption key must be securely deleted which is managed by the user and all data ever sent to persistent storage even with access to all secret keys. Any encryption key that decrypts any ancestor of the data's which corresponding vertex in the adversary's key disclosure graph. Encrypted data is only securely deleted when the user is unable to recover it. Adversarial knowledge and developed a graph mutation that maintains properties on

adversarial knowledge that allows straight forward provable secure deletion this is a reason of using graph theory [5].

3. Architecture

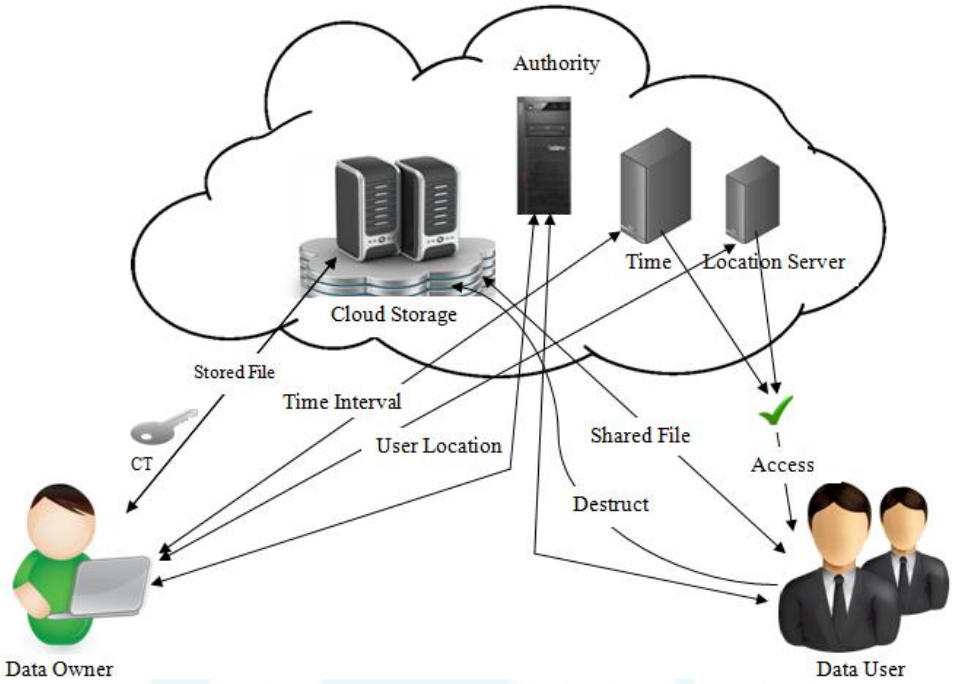

Figure 1: System Model of Proposed System

4. Proposed System

In the proposed system, we use two end users one is Data owner and second is data user. And there are three servers which are the Authority server, time server & location server. In system, first data owner and data user must have registered in the system. Authority of the data owner and data user is checked by the Authority server. In this, Data owner sends a file to the data user which is encrypted by the encryption algorithm and generates key. Alongwith this data owner specifies the time interval and location of the user for the security purpose. After this data owner stored the file on the cloud. Then data user Access the file by using the key after decrypting it. Data user can access file if the user attributes, time interval and location is matched. If this file is not access in the given time interval then the file is securely self destructed.

5. Conclusion

In the earliest systems, transformation of sensitive information on cloud is not more secure and file will not be destructed automatically. We develop a system in which we can use KP-TSABE scheme. Using this system we can secured our shared data. For that we used time and location parameters. These parameters prevent our data from third party user. From that system reliability is decreased. We also used self destruction for increased efficiency of our system. Our achievement is data shared securely as well as self destruct from the data user.

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] X. Liu, J. Ma, J. Xiong, and G. Liu, "Cipher text-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.

[4] K. G. Paterson and E. A. Quaglia, "Time-specific encryption," in *Security and Cryptography for Networks*. Springer, 2010, pp. 1–16.

[5] J. Reardon, D. Basin, and S. Capkun, "Sok: Secure data deletion," in *Proceedings of the 34th IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 1–15.