International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017(O)
Volume 1 Issue 5 (November 2014) ISSN: 2349-7009(P)
www.ijiris.com

Survey on Achieve Privacy Preserving using Multi-Key Approach in Cloud Environment

Poonam Patel
Department of Computer Engg, PICT, Pune, Maharastra, India.

Amar Buchade
Assistant Professor, Department of Computer Engg, PICT, Pune, Maharastra, India.

Abstract - In today's age, huge amount of data are being outsourced to cloud due to it's low cost service. User's data on cloud may contain personal information which may be caught or misused by third party or attacker without user knowledge or control. Privacy is an important issue for cloud computing in terms of legal compliance and user trust. In this paper, we detailed real world challenges of privacy preserving in cloud computing. The files stored in cloud storage by group of user's for indefinite period of time so it is easy for attacker to access user's private information. The concept of self destruction system is data and their copies are unreadable after user specified time without any user activity and also key is deactivated. Also this paper focuses on backup of data and managing the data on nodes. The system will identify the corrupted key and provide a new key to user's based on our algorithm.

Keywords - Data privacy, Self-Destructing data, Cloud Computing.

I. INTRODUCTION

Cloud Computing moves the application software and database to the large data centers, where the management of the data and services may not be trustworthy. This unique attribute creates many new security challenges. We only enjoy the full benefits of cloud computing if we address the real privacy and security concerns that come along with storing sensitive personal information in database [1]. As a more people start to take advantage of cloud. The cloud offers them so much like: (i) Limitless flexibility: Access of millions of different software and database and ability to combine different services. (ii) Better reliability: User have no worry about the crashing hard drives. (iii) Enhanced collaboration: It provides online sharing of information and application (iv) Portability: User can access data at any time whenever the connect to the internet (v) Simple devices: After data and software stored on cloud user need not a powerful computers.

There are some privacy problems address in the cloud computing: (i) Disclosure of sensitive information: when private data of user's like identification of user, Usage data, account number, secrete code are exchanging through the cloud services. (ii) Unauthorized access: This problem people getting inappropriate or unauthorized access to personal sensitive information in the cloud by taking advantage of lack of access control, security holes and so on. (iii) Dynamic environment: In this service interaction can be created in a more dynamic way than traditional methods. The personal sensitive information may move around within an organization or access organization boundaries.

Our paper is organized as follows: Firstly explanation of various privacy preserving techniques in cloud computing. Then self destructing data system in cloud and it's related works and last the conclusion.

II. DIFFERENT TECHNIQUES FOR PRIVACY PRESERVING

1. Identity Management [2]:

Authentication is the process of establishing confidence in user identities. Authentication assurance levels should be appropriate for the sensitivity of the application and information assets accessed and the risk involved. There are various authentication methods and techniques:

- User Password Authentication: It is the most general method that providing identification. When user accesses the resource, access control framework asks for the user name password provided to the user.

- Directory Based Authentication: This technique is Directory Based Authentication where user credentials are validated against the one which is stored in the LDAP Directory.

- Smart Card Based Authentication: Smart cards are small devices containing co-processors to process cryptographic data.

Authorization is an important information security requirement in Cloud computing to ensure referential integrity is maintained

2. Access Control Policy [3]:

Access control gives the authorization to the users to access resources that are publicly available to the users. The purpose of access control in cloud to prevent the access on object which is store on cloud by unauthorized users which enhance security in cloud environment. There are several scheme for access control in cloud environment.

Attribute-Based Access Control: In this scheme, User's identity consider as an attributes .Attributes use to generate a public key for encrypting data and as an access policy to control users' access.
Key-policy attribute-based encryption: In this scheme, cipher text associate with set of attribute, user decryption key associate with tree access structure. If it satisfy the condition then user decrypt the cipher text.
Cipher text-policy attribute-based encryption: In this scheme, role of cipher text and decryption key are switched. Cipher text encrypted with tree access policy chosen by encryptor. Decryption key created with set of attributes.

HASBE: This scheme, extended form of CP-ABE. Assign multiple values to the group of attribute in different sets. Organizes user attribute into a recursive set structure. It handle hierarchical structure of system users.

3. Access Management [4]:

Encryption:

Encryption is a process of encoding data or information in cipher text form which can not read by any user only authorized user can read it.

Encryption can be used in multiple places like,
▪ data in transit
▪ data at rest

When user's wants to original information or data, needs to decryption process on encrypted data.

4. Auditing [5]:

Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud.

III. Self-Destruction Approach to Achieve Privacy

A. Related Work

Self-destruct is a method that vanishes data automatically after it is no longer useful. There are number of application of self-destructing data. The first example is email. It can be leak via cloud service provider. One of the most important reason for exposing sensitive user's data that will be stored in cloud environment for a long time, which may not be control by user himself. Another example, self-destructing trash bins on desktops. These trash bins would preserve deleted files would self-destruct of time, but after a timeout the files would self-destruct [9].

M.Wei [7] proposed reliably erasing data from flash-based solid state drive. In this work, sanitizing the storage media to reliably destroy data is given which is an essential aspect of data security. The sanitizing individual file were effective and it increase complexity of SSD relative to hard disk drive.

R.Geambasu [9, 11] proposed vanish system for creating message that automatically self-destruct after period of time. Vanish system that meets the security challenges through novel integration of cryptographic technology with global scale, P2P and distributed hash table(DHT): DHT discard data older than a certain age. In this system, key is permanently lost and encrypted data is unreadable after data expiration. Vanish works by encrypting each message with random key and share of the key stored in large public DHT. Sybil attack may compromise the system. That is continuously crawling the DHT and saving the stored value before it's time out. S.wolchok[8] proposed defeating vanish with low-cost Sybil attacks against large DHT which overcome the drawbacks of vanish. The efficient Sybil attacks can recover the key to almost all vanish data object at low cost. There some changes in vanish implementation and the vuze DHT might make Sybil attacks somewhat more expensive, but it doubtful that it would make system sufficiently secure.

A.Rhea [8,9,11], contribution of this paper is provides more security. It proposed two countermeasures. It uses both open DHT and Vuze DHT so it provides maximum security. But if individual open DHT and Vuze DHT are insecure then obviously hybrid of that also insecure. L.Zeng [6] proposed a system to address the problem of vanish, called safe vanish, to prevent hopping attack, which is one kind of Sybil attacks [12], by extending the length range of the key shares to increase the attack cost substantially, and did some improvement on the Shamir Secret Sharing algorithm [14]. Also, improved approach against sniffing attacks by way of using the public key cryptosystem to prevent sniffing operation.

N.S Jeyakarthikka [15] proposed a system which works like SeDas to address the problem of vanish. The system prevent hopping attack. It protects the data privacy from attackers which may obtain data for legal or other mean. It perform self destruction approach without any action on user's part. It improves Shamir Secrete Sharing algorithm, so it improves key split up in SeDas using a Short Secrete Sharing. But Short Secrete Sharing is not able to identify the corrupted or malicious keys.

There are the number of drawbacks in previous systems like, the SeDas not able to manage data on nodes, User's can't able change the value of TTL after submitting it one time. There are two major drawbacks in SeDas: the first one is, all parts of secrete key after splitting stored on metadata server. Metadata server is also a type of hacker. And Second is very important concept which lack in SeDas is securely share the data file among the dynamic groups of user's.

B. Proposed System

The proposed work provides a more privacy. The typical SeDas is only preserve privacy for single user. It is not work for group of user's or multi-owners for file. If group of user's upload a single file and after some period one member from group left the group then it is So in propose work over the drawbacks of SeDas and also improve key splitting algorithm and key storage scheme.

Fig 1. Shows the System architecture. There are three modules in this architecture: (i) Metadata Server: It is responsible for user management, server management, session management. (ii) Self-Destruction System: Application node is used to store the service of self destruction system. (iii) Storage Nodes: It contains two subsystem. It is key value store subsystem that is based on Object storage component The data stored on storage nodes in a round robin fashion. The purpose of this technique

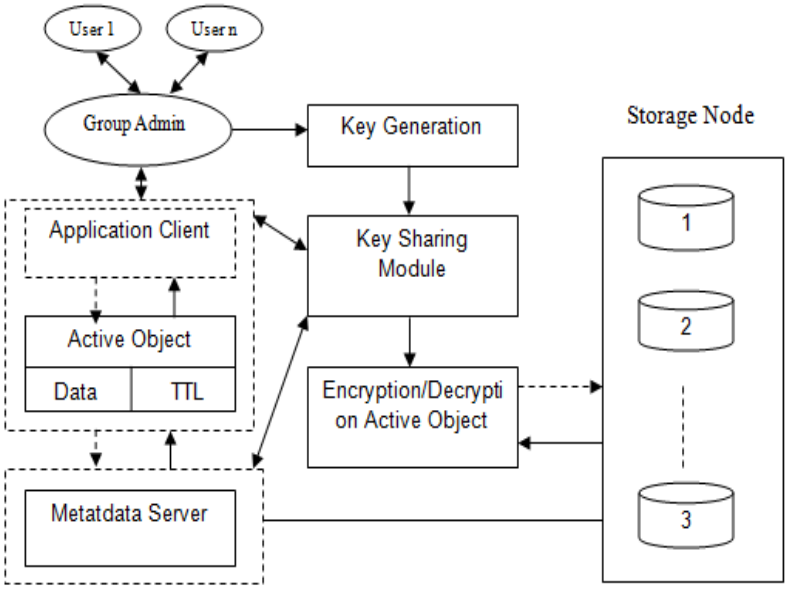

Fig 1: System Architechture

1. Data Process:

There are two different processes: uploading and downloading.

(i) Uploading File:

There are three arguments for uploading a file: file, Key, TTL(Time-To-Live). The user upload a file to storage system and stores some key parts on client node and some key parts on metadata server . The process use a user-defined encryption algorithm.

(ii) Downloading File:

User's are requested to download file which is stored in data storage system. Only those user have relevant permission can download file. Before decryptin,g client should try to get key parts from storage nodes and combine with key parts which is on client nodes. The decryption process of the file is possible if and only if all the decryption key

shares that satisfy minimum threshold count. If the time parameter of file expire then client cannot get enough key parts to rebuilt original key because after time expire of file, the key is deactivated.

User Revocation: The user revocation is the process of removal of a user from participating in the group on a basis of certain conditions. Revocation process is authorized to perform by Group Admin through a publicly available revocation list. If the login of the specified user matches with the details of revocation list then access denied to that particular user.

2. Self Destruction System:

This is a improved module of SeDas. The basic concept of self destruction module is the key and user's sensitive data are inaccessible after some time without any external user's activity. It's providing privacy to the user's sensitive information which is stored on cloud environment. To maintain security of cloud file's and privacy regularly deletion of unwanted files is needed. This system delete unwanted files automatically when the specified time period for key sharing by data owner has been expired. In which typically number of operation like key splitter and key combiner.

(i) Key Splitter:

Key is a secrete for accessing a user's data from cloud. Key is necessary for encrypting and decrypting data. Each file stored on cloud is encrypted using a random key. Many times key is hacked by unauthorized user and they are accessing original file of legitimate user without the permission of original users. To achieve privacy of user's data on cloud there is a need of maintaining a secrecy of key.

Key splitter is a concept for maintaining a secrecy of key. In which split the original key in number of parts and stored key in user node and metadata server.

Shared_key = {user_node, server_node}

There are three parameter to split the key:

Key_Splitter_function = SplitAlgo(n, k, key);

Here, n is key storage nodes, k is a number of parts of original key, key is a original key.

(ii) Key Combiner:

Key combiner is a concept used at the time of download file because the downloaded file from cloud is not in original form, it contained a file in encrypted form. So to optain original file user wants to decrypt file but key is splitted and stored on different nodes So it's necessary to collect and combine original parts of key. There is a no need to combine all parts of key, if only some parts of key are collect which satisfied number of threshold value then also user can access data**.** Key combiner is technique to collect all parts of original key and combine to obtains key for decryption operation.

IV. CONLCUSION

There is millions of user's are stored large number of sensitive and important data in cloud environment. Data privacy of sensitive data has become increasingly important. There are number of techniques available for maintaining a privacy like authentication and authorization, access control policy, auditing and many more. The existing techniques are not provided much privacy. They are gives some place or leakage for attacker/hackers to access the users data. In authorization and authentication only verify the identity of user's and their permission but some hacker's can act as a legitimate user and access the data likewise all techniques have some limitation and drawbacks. From above study, we will analyze the drawbacks and limitation of existing techniques and study to overcome those points in future using self destruction of data and achieve privacy of key in group of user's storing and sharing in a dynamic environment.

REFERENCES

1. J.Wang, Y.Zhao, S.Jiang, J.Le, "Providing privacy preserving in cloud computing" *China.*
2. Abdelmajid Hassan Mansour Emam, "Additional Authentication and Authorization using Registered Email-ID for Cloud Computing" *(IJSCE) ISSN: 2231-2307, Volume-3, Issue-2.*
3. Zhiguo Wan, Jun'e Liu, and Robert 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, APRIL 2012.*

4. Safiriyu Eludiora1, Olatunde Abiona, Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime, Lawrence Kehinde, "A User Identity Management Protocol for Cloud Computing Paradigm" *Int. J.Communications, Network and System Sciences, 2011, 4, 152-163.*
5. Bhavna Makhija, VinitKumar Gupta, Indrajit Rajput, " Enhanced Data Security in Cloud Computing with Third Party Auditor*" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013 ISSN: 2277 128X.*
6. L.Zeng, S.Chenting, Q.Wei, D.feng, "SeDas: A Self-Destruting Data System Based on Active Storage Framework" *IEEE TRANSACTIONS ON MAGNETICS, VOL.49, NO.6, JUNE 2013.*
7. M.Wei, L.M.Grupp, F.E.Spada, S.Swason, "Reliably Erasing Data from flash based solid state drives" *in Proc. 9th USENIX Conf. FAST, USA.*
8. S.wolchok, O.S.Hofmann, N.Heninger, E.W.Felten, J.Alex Harderman, C.J. Rossbach, B.Waters, E.Witchel," *Defeating vanish with low-cost Sybil attacks against large DHEs," 2009.*
9. R.Geambasu, T.Konno, A.Levy, H.Levy, "Vanish: Increasing data privacy with self-destructing data," *in Proc. USENIX security Symp, Montreal, Canada, Aug. 2009, pp.299-315.*
10. Y. Zhang and. D. Feng, "Active storage framework for object based storage device," *in Proc IEEE 20yh Inc Conf (AINA), 2006.*
11. A.Rhea, B.Godfrey, B.Karp, J Kubiatowicz, "OpenDHT: A Public DHT Services and Its Uses", *Intel Research.*
12. J.R. Douceur, " The Sybil attack, *" in Proc. IPTPS '01: Revised Papers from the first Int. Workshop on Peer-to-Peer System, 2002.*
13. A. Shamir, "How Secrete Share a secrete," *Commun. ACM, vol. 22, no. 11, pp.612-613,1979*
14. J. L. Dautrich and chinya V. Ravishankar, "Security Limitation of Using Secrete Sharing Data Outsourcing, " *University of California.*
15. N.S Jeyakarthikka, S.Bhaggiaraj, A.Abuthaheer, "Self Destructing Data System Based On Session Key" *International Journal Of Scientific & Technology Research Volume 3, ISSUE 2, FEBRUARY 2014, ISSN 2277-8616.*

