Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-7, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Automatic Data Destroy Based on Specified Time in Cloud Computing

Ms. Vikalpa Landge[1] & Prof. S. P. Pingat[2]
[1]ME Computer, Department Of Computer Engg, SMT.Kashibai Navale College Of Engg, Savitribai Phule,Pune University.
[2]ME Computer, Department Of Computer Engg, SMT.Kashibai Navale College Of Engg, Savitribai Phule, Pune University.

Abstract*: In recent- era cloud computing is technology mainly used to store data and sharing data amongst multiple users. Cloud services provide flexibility and large storage space, so users store their secure data in cloud. But cloud is vulnerable to security threats so unauthorized user can access secure data of user. The data stored on cloud can be sensitive and more important for user. The data which is stored over cloud resides on multiple sites for undefined time over cloud. In order to solve this security issue, personal and sensitive data stored over cloud should be deleted after particular period of time. Data should be stored securely over cloud so no unauthorized user can access the data. To achieve this functionality, system proposed here is Key-policy attribute-based encryption with time-specified attributes (KP-TSABE). In this scheme, every cipher text is labeled with a particular time of interval while private key is associated with a time instant. The encrypted text can only be decrypted within particular user specified time and attributes associated with encrypted text matches with key's access structure. This scheme provides security by authenticating/authorizing user and by providing the fine-grained access control in user specified time. Sensitive and private data stored in cloud is self-destroyed with all its copies from cloud in user specified time period. This KP-TSABE scheme proposed here solves all the security problems which are there in existing system.*

1. Introduction

In recent era, cloud services are used by many users as well as industries. Cloud provides large amount of space to store and share data so that it can be available in any period of time over network when user requires it. Cloud provides such services in very low cost. Compared to traditional technologies, cloud has many specific features, such as its large scale and the fact is that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized [1]. Users can store sensitive data as well as share pictures, videos, audios or any file over cloud so that it can be accessed on demand service.

The data which is stored over cloud has many security issues; it is vulnerable to various security threats. User can store any sensitive information over cloud. Such information can be saved with multiple copies over cloud for ease of searching. In such case, privacy issues of user's shared data come into picture. Privacy breaches may create many problems to cloud users. Cloud Users always expect high level of protection for their sensitive data. Violation of protection leads to user's dissatisfaction [2].

To tackle this privacy issue, there should be a system which gives administrative rights to user for storing and sharing of file. So that user can get single access and can provide rights for accessing the data. Also cloud stores data for infinite time; it is not feasible for user to delete data each time which is not required for infinite time. There should be some mechanism which deletes data over cloud on time basis that means any file can be available for user for particular period of time. After that time, access to the authorized data should be revoked for everyone - including the legitimate users of that data, the known or unknown entities holding copies of it, and the attackers [3].

One of the methods to delete automatically stored user data over cloud is self-destruction of data. Self-Destruction data implemented by encrypting data with generation a key and that information is needed to reconstruct the decryption key with one or more third parties [4]. With self-destructing data, users can regain control over the lifetimes of their Web objects, such as private messages on Facebook, documents on Google Docs, or private photos on Flicker [3]. There are some systems proposed for the mentioned issue named as Vanish [3], SeDas [4]. Vanish linked the cryptographic techniques with global scale, P2P and distributed hash tables. Characteristics of P2P are challenges of Vanish, duration of key survival is also not known in Vanish, attack like Sybil attack and hopping attack are possible in Vanish.

Data stored over cloud in encrypted format and when it is retrieved then it gets decrypted for accessing. One disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data at a fine-grained level [9]. There is one concept called Attribute Based Encryption (ABE) is a type of public key encryption in which the secret key of a user and the cipher text are dependent upon attributes which was proposed by Sahai and Waters [11]. In an ABE system, a user's keys and cipher text are labeled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key [9].

2. Literature Survey

Dr. Arockiam L et al has focused on issues related to cloud. Paper mainly focuses on the issues related to data privacy and other protection issues in cloud computing. Privacy is defined as a fundamental human right related to the collection, use, disclosure, storage and destruction of personal data (Personally Identifiable Information-PII). The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Charted Accountants (CICA) define that it is the right and obligation of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information. Privacy is the protection of appropriate use of personal information of cloud user. [1]

Keiko Hashizume et al has analysed security issues in cloud and as per the analysis, Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with the use of cloud computing. In Cloud computing Security is major factor for transferring data from one to another. This paper presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. In this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing.
Mutual Authentication technique used here for isolate the side channel attack in the cloud computing. Virtualization which al-lows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. [3]

P. Muralikrishna et al has proposed the system which involves a design of a pre-distribution algorithm using a deterministic approach. Deterministic approach is a process of determining the keys before placing them within network. A key for pre-distribution algorithm using number theory with high connectivity, high resilience and memory requirements is being designed by implementing a deterministic approach. [2]

N. Ramakalpana et al have presented an Asymmetric Cryptography in cloud computing i.e. encryption and decryption process. RSA algorithm is used for establishing security in the internet in terms of encryption and decryption. Its strength is its computational complexity. It is known for its security based on finding the prime factor of very large numbers. [4]

Kshama D. Bothra et al have implemented the SeDas system. Application client connect through metadata server. In metadata user management, server management, session management, key management. This paper creates multiple nodes for performing the sedas application. Users can perform operation like uploading, downloading or any activity in cloud server then privacy is must for transferring the shared data. So this paper implementing Shamir's Algorithm for performing encryption and decryption operation. [5]

3. Problem Statement And Proposed System

A. Problem Statement

In recent era cloud services are used to store as well as share user data. This shared data can be any sensitive, private data of user. But cloud is vulnerable to various security threats. User data can be accessed or misused by unauthorized user. Also data resides on cloud for infinite time. Due to this data gets more vulnerable to security threats

There are various techniques evolved to resolve the security issues in cloud. A Secure self-destructing of electronic data (SSDD) [10] is one of the systems which is improved version of Vanish [7] system but this systems drawback is that SSDD done not allow user to determine expiration time of the private data. This time is limited by DHT network. The Vanish, SSDD and other schemes are vulnerable to Sybil attack from DHT network. Due to this unauthorized users can easily access secure and private data of user which leads to serious security problem.

B. Proposed System

There are lots of security problems in cloud data access. In this paper it is considered how to resolve all the security problems which user faces. Also how user can specify expiration time for cloud data on which data gets self destructed with all its copies over cloud. It supports user defined authorization period in which fine-grained access control is provided over the period.

For achieving security in cloud data sharing, Key Policy Time Specified Attribute Based

Encryption (KP-TSABE) technique is used in this system. By using KP-TSABE scheme author of cloud data can do following things.

a. *Author can provide fine-grained access to the entire authorized user having cloud access.*
b. *Author gives access to user for a specific time period. After that time no user (even if it is authorized or it is unauthorized) can access data which is shared by the user.*
c. *Data is shared over cloud for the particular time of period which is specified by the author. The datawhich is shared is in encrypted form so that no one can read the data without decrypting it.*
d. *When user specified time expires, shared data gets self-destructed. While deleting data, this system not only delete original data but also all the copies of data which are resided over cloud.*

In this system user can specify time for authentication as well as for self-destruction of data and also this system is not vulnerable to Sybil attack as it does not use DHT network for encryption and decryption of data.

4. Architecture Of Proposed System Model

The main task of this system is to provide fine grained access in authorization time period with the self destruction of data after expiration of access time. System model of KP-TSABE model is as shown in following Fig 1.

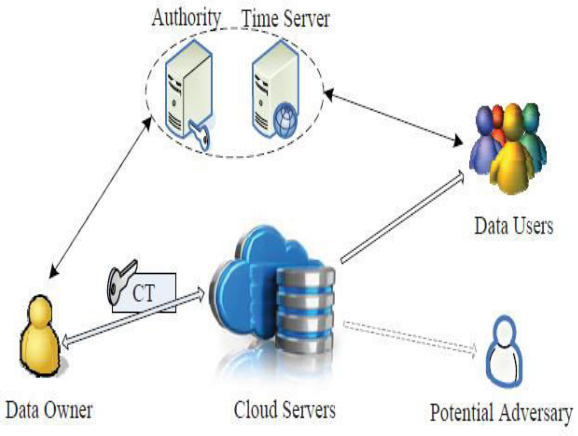

Figure1. System Model of KP-TSABE

1) *Data Owner*: This is user who shares data or files, containing private information with other data users. Data owner stores his/her data over cloud so that other data users can access data from cloud.
2) *Authority*: Task of authority is to generate, provide and manage private key of users. Authority is an entity which is trusted by all the other users present in the system.
3) *Time Server*: This server has responsibility regarding time specification. It does not interact with any other entity in the system.
4) *Data Users*: These are the users who have passed through authentication and access the data which is shared by the data owner. All the data users are able to access shared data by authentication and within authorization period only.
5) *Cloud Servers*: There are the servers where data owner shares his/her data. Cloud servers have almost unlimited storage space. Cloud servers store and manage stored data so that it can be easily available to users who are accessing cloud.
6) *Potential Adversary*: It is an entity which declares attribute sets for challenger. This means adversary generates repeated private keys and to access attribute structure.

5. Mathematical Model

We have created system in .Net. Data is stored in SQL Server 2012 DB and also used Sql Server reporting services. We have created a web application with local server and reports deployed in local report server

Web application that communicates with local Server.

Mathematical Model:

System Description:

Input:

Upload file ()

U : Upload file on cloud.

E : Encryption File.

T : Time for shared file.

D : Decrypt value for each file.

Output:

Check Encryption file on cloud storage and time specified for the file

Input:

Function destruct data(id,file,time)

ID : unique id for each file.

File : Check file on cloud.

time :time specified to file for self destruction

Output:

Data will be self destroyed after specified time.

6. Implementation Strategy And Experimental Setup

To implement this system KP-TSABE scheme is used in this paper. KP-TSABE is implemented by using four algorithms: Setup, Encrypt KeyGen and Decrypt key.

- *Setup*: This algorithm takes security parameter and attribute as input and outputs the system public parameters and master keys. As this algorithm is run by Authority, so after getting output, Authority provides parameter publically by keeping master keys secrete.
- *Encrypt*: This algorithm generates cipher text of shared message/data by owner. This cipher text contains encrypted message/data with user specified time interval.
- *KeyGen*: This algorithm takes master key (generated in Setup step), access tree and the time set as input. Each attribute in access tree associated with a time instant for generating output. Output of this algorithm generate private key containing access tree.
- *Decrypt*: Input to this algorithm is cipher text (generated in Encrypt step) and private key (generated in KeyGen step). When all the attribute in access tree satisfies specified time then this algorithm decrypts the cipher text and generate plain text. This plain text is nothing but the original message.

.

7. Conclusion

In this paper, we proposed system for Automatic Purging of Secure Data Based on Specified Time in Cloud Computing
for dynamic group data sharing. Since shared data items in dynamic groups remains for infinite time in the system will considerably reduce the security and privacy of system with increased complexity in managing data files. Hence, in this self-destruction system all files will be removed automatically if those are no more needed. Also, the time period for sharing can be explicitly fixed by data owners while uploading the files itself. We strongly believe that the system will reduce complexities in managing old data files and thereby increasing possibilities in reducing security and privacy issues.

8. References

[1] Dr. Arockiam L[1], Parthasarathy G[2] and Monikandan S[3],"Privacy in Cloud Computing : A Survey", Natarajan Meghanathan, et al. (Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 321–330, 2012.

[2] P.Muralikrishna1, S. Srinivasan2, N.Chandramowlis-waran3, "Secure Schemes for Secret Sharing and Key Distribution Using Pell's Equation", International Journal of Pure and Applied Mathematics, Volume 85 No. 5 2013.

[3] Keiko Hashizume[1], David G Rosado[2], Eduardo Fernández-Medina[2] and Eduardo B Fernandez[1], "An Analysis Of Security Issues For Cloud Computing",Hashizume et al. Journal of Internet Services and Applications 2013.

[4] N. RamaKalpana[1], R. Santhosh[2], "SeDas Self - Destruction Data System for Distributed Object Based Active Storage Framework ", International Journal of Software and Web Sciences, 7(1), December 2013-February 2014, pp. 94-100.

[5] Kshama Bothra[1], Sudipta Giri[2], "Enhancing Security in Cloud by Self-Destruction", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 9, September 2015.

[6] John Bethencourt, Amit Sahai, Brent Waters, "Ciphertext-Policy Attribute-Based Encryption".

[7] Roxana Geambasu Tadayoshi Kohno Amit A. Levy Henry M. Levy, "Vanish Increasing Data Privacy with Self-Destructing Data".

[8] J. Xiong, Z. Yao, J. Ma, F. Li, and X. Liu, "A secure self-destructing scheme for electronic data", Chinese Journal of Computers, vol. 37, no. 1, pp. 139–150, 2014.

[9] Qinyi Li[1], Hu Xiong[1,2], Fengli Zhang[1], and Shengke Zeng[1], "An Expressive Decentralizing KP-ABE Scheme with Constant-Size Ciphertext", International Journal of Network Security, Vol.15, No.3, PP.161-170, May 2013.

[10] Nuttapong Attrapadung[1], Benoit Libert[2], Elie de Pana-fieu[3], "Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts".