ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Secure Data Self Destruction Scheme Using Two Level Security on Cloud

Navnath Bhosale, Sumeet Karn, Sunil Moosad, Mayur Pare, Rajesh Lomte

Student, Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India

Student, Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India

Student, Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India

Student, Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India

Assistant Professor, Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India

ABSTRACT: Nowadays, almost all corporate as well as government organizations uses public cloud services. These public cloud service providers maintain and manage the storage of data. With increase in use of these services there is always a risk of data breach. To overcome the flaws in the system we propose two level security on cloud. The first level of security is KP-TSABE (Key Policy-Time Specified Attribute Based Encryption) scheme, which ensures the confidential data is available only to a specific user in a specified time limit. The time limit will be set by the data owner and specifies the attributes of the user which will be matched by the authority during the time of accessing the data. The second level of security is fragmentation of data stored in cloud servers. For this purpose we use T-coloring graph mechanism to select a node in which the fragments of data are to be stored. The T-coloring graph ensures that the fragments are separated by a certain distance. Fragmentation is a non-cryptographic way of securing the data, due to which the system is relieved of computationally expensive methodologies. A slight performance was also observed for fragmentation and retrieval of data.

KEYWORDS: KP-TSABE policy, non-cryptographic way, fragmentation.

I. INTRODUCTION

The number of cloud services being used in enterprise is growing daily. Cloud applications are easy for users to buy and require minimal effort to get up and running. It provides users and enterprises the capability of storing and processing their data in either privately owned or third party data centers. But the downside of this public cloud is that management of data storage is not in the hand of business enterprises. The shared data can be user's sensitive information (for e.g. personal profile information, financial details, and other important data) must be well protected. That's why the security and privacy becomes big challenge in cloud computing. So it is essential to provide comprehensive solutions against these circumstances.

One of the best ways to secure data is to provide specific predefined authorization period and to give fine grained access within that period. And the sensitive data should be self-destroyed after that expired time span. Key Policy-Time Specified Attribute Based Encryption (KP-TSABE) policy[1] is used for this purpose. Sometimes owner of data wants to share their information with particular user, then Attribute Based Encryption (ABE) technique plays vital role; this technique has significant properties based on public key encryption which provides one-to-many encryption. So data owner sets specific attributes for that particular user. After the validation of these attributes, user gets grant for accessing data. Then only that user can access.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

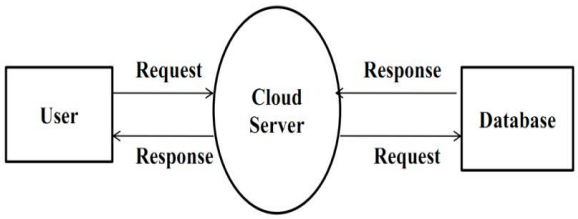
Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

II. RELATED WORK

The system consists of four parts, Cloud Server, Users, Administrator, Authority and Time Server. Amongst these units Administrator and Users are provided with GUIs. In this system the users request for the files they want and after authenticating the user the administrator will upload the file. The file is then encrypted during the uploading process. This file is then sent to the cloud server. Thereafter the cloud server has a fragmentation algorithm called DROPS(Division and Replication of data in cloud for Optimal Performance and Security)[4] which is used to divide the file into specified number of partitions. These partitions are then stored into different nodes in the file server of cloud. To decide which nodes are to be selected for storage T-Coloring graph is used. The existing system includes following modules:

1) Cloud Server:- The cloud server provided by cloud service provider, it can be a third party system. That's why it must be secure enough to store confidential files as well as organization's private information. In existing system cloud is also used for storing and sharing purpose.



2) Data owner:- Owner of data can be of same organization or different. Data owner used to upload their information on cloud server and provide the attributes of particular data user who is going to use that information. Owner of data sets some parameters to validate and authenticate data user.
3) Data User:- Firstly user has to register in the system where he fill all details about him, it can be his organization's name, designation etc. When data owner used to upload the file he will first use these parameters to set. After that at user side all these parameters are going to match and after validation that user will get access of it.
4) Authority and Time Server:- Authority manages all records of users. It is responsible to provide validity of all activity execution. Authority is also responsible for generating the keys for authenticate the users; the keys are of types private keys or public keys. Time server used to set time span in which file is only accessible. After the expiration of time that file won't be accessible.
5) Potential adversary:- It is also called a polynomial time adversary and described in security model of the KP-TSABE scheme.

Formal model of KP policy:-

The KP-TSABE policy is described by a collection different scheme as such as follows:

Setup(1κ,U):- This algorithm is run by the Authority and takes as input the security parameter 1κ and attribute universe U, generates system public parameters params and the master key MSK. The Authority publishes params and keeps MSK secret to itself.

Encrypt(M, params, S, TS):- Given the public parameters params, the shared message M which the owner wants to encrypt, the attribute set S and the set of time intervals TS in which every element in TS is associated with a corresponding attribute in S. This algorithm generates the ciphertext CT which is associated with the fuzzy attribute set S.

KeyGen(MSK,Y,T′):- This algorithm takes as input the master key MSK, the access tree Y and the time set T′. Every attribute x in Y is associated with a time instant tx T′. It outputs a private key SK which contains Y.

Decrypt(CT,SK):- This algorithm takes as input the ciphertext CT and the private key SK. When a set of time-specific attributes satisfies Y, it is able to decrypt the ciphertext and return the plaintext M.

To form a basis for the KP-TSABE scheme, we introduce the following concepts [2].

(1) Authorization period:- It is the predefined time interval which is set by data owner who uploads their

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

confidential data. That period is valid for accessing that ciphertext to decrypt it and gain information. After that period files won't be accessible.

(2) Expiration time:- It is threshold time interval which is pre-defined by the data owner. The shared data can be accessible only in authorization period after that it won't be. It is called as expiration time of that data.

(3) Full life cycle:- It is a time span from the uploading of confidential data, authorization period till expiration time.

System descriptions of the KP-TSABE scheme:-

1) In system initialization phase, firstly data owner uses security parameter κ and attributes U, and passed it to Setup(1κ,U) which generates params which is system parameters and a master key i.e. MSK.

2) Data owner selects an attribute set S for message M and time interval set TS for S. Then all these attributes passed to Encrypt (M, params, S, TS) to encrypt message M which generates ciphertext CT. And finally this CT is sent to cloud server.

3) KeyGen(MSK,Y,T′) is used to generate the private key SK and sends it to the user, by entering this private key file is accessible to particular user. By entering private key Decrypt(CT,SK) invokes and used to decrypt CT to obtain the data M.

4) Data will be self-destruct after the expiration of current time instant. If data user has private key but time expires then he won't be accessed that data. It means that cipher text CT will not decrypted in polynomial time.

III. PROPOSED ALGORITHM

In this paper we propose two level security using KP TSABE policy and fragmentation of data. The security will be enhanced as we are merging two concepts namely KP TSABE policy and fragmentation. KP TSABE is implemented by Authority. KP TSABE improves access level security for users. Fragmentation is implemented on the file server. It allows fragmentation of data and storage at non contiguous locations on file server thus enhancing storage level security.

Using KP TSABE, the access of the files will be limited to intended audience based on their attributes like user's name, designation, company name. The Authority will keep track of all the data users and data owners. Thus only registered users will be able to upload or download the files. Encryption is done by AES algorithm by using the private key which will be provided by the Authority. In order to do decryption the private key will be needed by the data user , the private key will be provided to the data user by the Authority using Email service. The data user will get private key only if the data user has rights to access the requested file. It is responsibility of the Authority to check whether the user is valid user for the requested file. Also the data user will get the private key if he request the file within the time intervals specified by the data owner. Thus using KP TSABE, the file gets decrypted only when attributes and time intervals are matched correctly. This policy thus improves access level security of the system.

Fragmentation is done by dividing the encrypted file into fragments and then storing these fragments on file server/cloud[4] .There are various methods for doing fragmentation. Here we are proposing a basic method. The given file is fragmented into parts and each part is stored in a randomly selected location on the cloud. The location where the fragment is stored is recorded in the database. Thus when the user wants to download the file, database will give number of fragments that file has along with their locations on the cloud. Thus, maintaining a database for the locations of the fragments will help us in find the fragments on the cloud and it will be useful to merge all the fragments to get the encrypted file. This encrypted file will be then decrypted using private key provided by the Authority. Thus this technique will enhance the storage level security of the cloud. Thus even if the file server is compromised then also data will not be compromised as it was encrypted and fragmented.

The following figure shows various components of proposed system. It has data owner , data user , cloud server , Time server , Authority and fragmentation entity. These entities are the functional entities of the proposed system. Thus these entities must be mandatory to be implemented.

The non functional aspects of the system like efficiency, performance , access time etc. are also very important and they need to be improved by choosing fast algorithms for encryption, decryption. Also the hardware on which the system is running is also important as it will improve efficiency of the system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

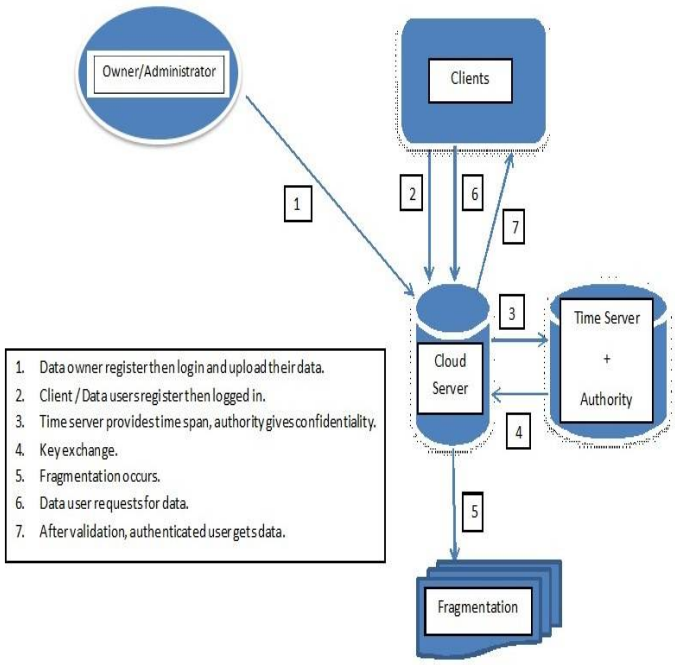
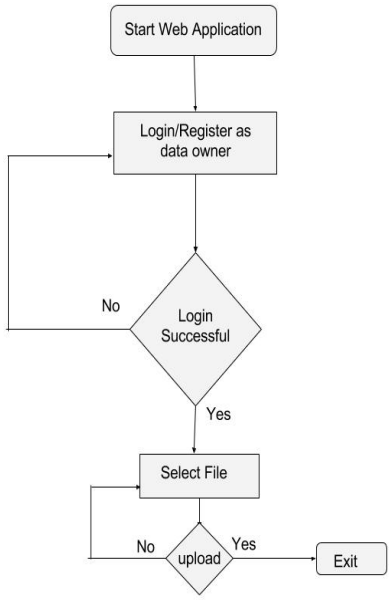


Fig: Architecture of system



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

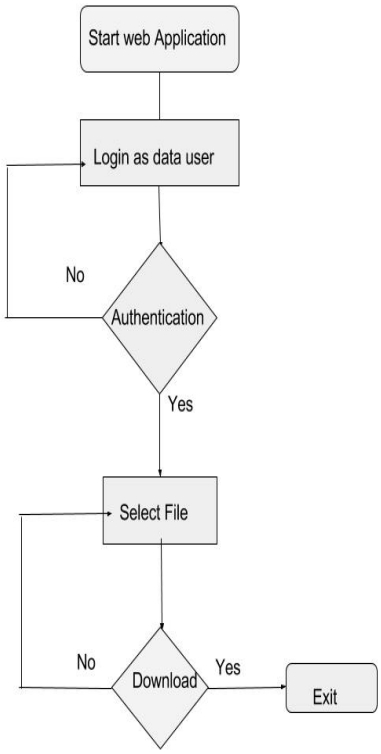
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Uploading is basic task which need to be done. We just have to login and select the required file and remaining things like fragmentation will be done by the functionalities implemented by the system.



In order to download file again the user has to login and select the required file to download. Merging the fragments and all will be done by the functionalities that are implemented.

IV. ALGORITHMS

Algorithm For Encryption/Decryption (AES) :

Advanced Encryption Standard (AES): It is a symmetric encryption algorithm. AES was designed to be efficient in both hardware and software. The implementation of AES in products intended to protect national security systems . Thus we have used AES algorithm for encryption as is fast and secure algorithm. We have used java packages to encrypt data using AES algorithm. It is ease to use these packages for encrypting using AES algorithm. Thus encryption becomes easy using java classes and packages , decryption is also done in similar manner[6].

Algorithm For Fragmentation of File:

1) Divide the file into four parts as A,B,C,D as names of fragmented file .
2) Each fragment is mapped to a node by randomly selecting a node.
3) Record the mapping detail in a table .
4) Put the fragments in their mapped nodes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Algorithm for Uploading File:
1) Login as data owner using GUI .
2) Choose file to be uploaded .
3) Set data user attributes like name, designation, time, etc.
4) Private key is generated .
5) File is encrypted using AES algorithm.
6) File is fragmented (using fragmentation method)
7) Fragments of file are stored at different locations in cloud.

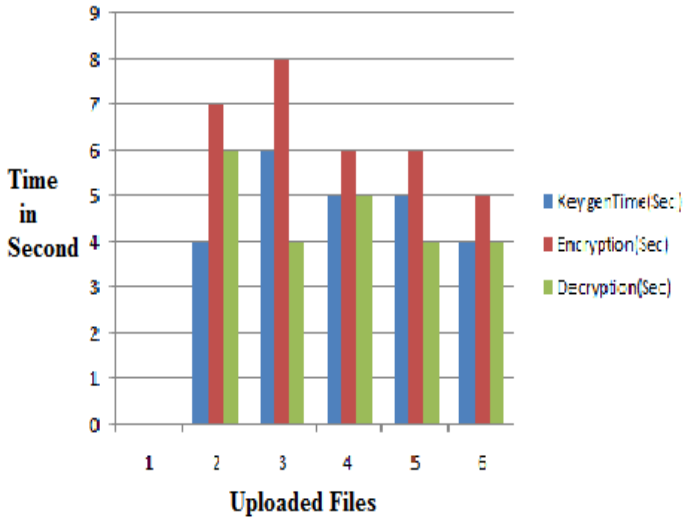
Algorithm for downloading File:
1) Login as data user using GUI.
2) Select file which need to be downloaded.
3) Request file from authority.
4) Authority will provide private key to data user using mail service if time is matched.
5) Merge the fragments from different nodes .
6) Decrypt the file using decryption key.
7) Download the file from cloud.

V. EXPERIMENTAL RESULTS

The web application is developed such that it simulates a cloud server with client server capabilities. Our testing showed that the cryptographic computations took very small amount of time with encryption consuming more time than the decryption of a file.

In the proposed system, when uploaded button is first pressed it encrypts the file. This file is then divided into parts of predefined size. This alleviates the system of dividing the data into different sizes of data by dynamically taking input from user as proposed in [4]. This ensures faster system execution and also retrieval of data.

The following graph shows the various execution times for key generation, encryption and decryption of files of different sizes using AES algorithm:



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Following is the representation in tabular format:

File	Key genTime(Sec)	Encryption(Sec)	Decryption(Sec)
1	4	7	6
2	6	8	4
3	5	6	5
4	5	6	4
5	4	5	4

The use of KP-TSABE scheme along with fragmentation of data allows the confidential data to be provided with more security. The organizations using the two level security scheme proposed in this system will not have to be concerned about the security. The use of AES algorithm with SHA-256 hashing algorithm is the best combination to ensure confidentiality and integrity[3].

VI. CONCLUSION AND FUTURE SCOPE

In this paper we proposed two level securities on cloud by KP-TSABE scheme and Fragmentation where we used to store this data on non-contiguous memory location. This method provides better security for confidential data storage. The KP-TSABE scheme shows that the confidential data is accessible only to the authenticated user. Fragmentation of data shows that no meaningful data is possible to be retrieved even if a single node is attacked or private keys are available to the adversaries.

Currently, the proposed scheme uses only single CPU for complex computations like encryption, decryption. In future the cryptographic computations can be done using GPUs. This ensures faster cryptographic calculations. Also we can implement reinforcement learning to make the system learn about the importance and priority of confidential data using the past behavior of owner and user interaction.

REFERENCES

[1] Jinbo Xiong, Ximeng Liu, Zhiqiang Yao, Jianfeng Ma, Qi Li, Kui Geng, and Patrick S. Chen, "A secure data self-destructing scheme in cloud computing," *IEEE transactions on cloud computing* vol:pp no:99, 2014

[2] 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.

[3] K. Kasamatsu, T. Matsuda, K. Emura, N. Attrapadung, G. Hanaoka, and H. Imai, "Time-specific encryption from forward-secure encryption," in *Security and Cryptography for Networks*. Springer, 2012, pp. 184–204.

[4] Mazhar Ali, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, and Albert Y. Zomaya, "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security," IEEE Transactions on Cloud Computing, 2015

[5] Nilesh R. Patil, Rajesh Dharmik "Secured Cloud Architecture for Cloud Service Provider," World conference on futuristic trends in research and innovation for social welfare, 2016

[6] Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy, "A Secure Cloud Storage System Combining Time-based One Time Password and Automatic Blocker Protocol," *IEEE*, 2015