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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Access Privilege Control and Storage Optimization Using Attribute Based Encryption in Cloud

Soni Kumari, Dr.Sulochana B. Sonkamble

PG Student, Department of Computer Engineering JSPM NTC, Narhe Rajarshi Shahu School of Engg.& Research, Pune Maharashtra, India

Associate Professor, Department of Computer EngineeringJSPM NTC, Narhe Rajarshi Shahu School of Engg.& Research, Pune, Maharashtra, India

ABSTRACT: Most of the organizations and individuals preferring clouds nowadays. Cloud is currently a most popular option for storage and shared resource provider. Because of low cost, large share resources and high efficiency, the cloud is gaining more popularity.With high demand and supply, the cost of the infrastructure of cloud system increases. Another concern is security. When cloud infrastructure store and process data on their servers for multiple users, then it cause an effect on security privacy and infrastructure.Many works are done in content privacy and access control for a particular file in the cloud. Privilege control and the identity privacy is ignored. Also, there is very less work on data deduplication within the same server. So, this paper focuses on a full anonymous privilege control as AnonyContol and AnonyControl-F respectively. The technique used in this paper not only ensure the data privacy and accessibility but also prevent the duplication of data in a server with identity protection. It also prevents the identity leakage that providing identity privacy. When same data is uploaded by multiple users and share among them self than it increases data duplication in cloud storage, hence lead to less storage. A combination of data indexing technique (Hashing algorithms) along with identity-based encryption algorithm (ABE) is used for this reason. This gives secure optimization of data in the cloud and provides security to users accessing the same data.

KEYWORDS: Anonymity, Multi-authority, Data Encryption standard, Attribute-based Encryption.

I. INTRODUCTION

Most of the organizations and individuals preferring clouds nowadays. There is so many cloud storage provider available to store your data. Cloud is currently a most popular option for storage and shared resource provider. And the use of cloud is increasing day by day. Because of low cost, large share resources and high efficiency, the cloud is gaining more popularity. With high demand and supply cost of the infrastructure of cloud system increases. Another concern is security. When cloud infrastructure store and process data on their servers for multiple users than it cause an effect on security privacy and infrastructure. Many works are done in content privacy and access control for files in the cloud. Privilege control and the identity privacy was ignored most of the time. This leads to the security issue, as other users within the same cloud can access data. Also, there is very less work on data deduplication on the cloud. That means if same data is coming, again and again, the current system will simply store it again. When same data is uploaded by multiple users and share among other, then it increases data duplication in cloud storage hence lead to less storage. So, this paper focuses on a full anonymous privilege control as AnonyContol and AnonyControl-F respectively. The techniques used in this paper not only ensure the data privacy and accessibility but also prevent the duplication of data in a server with identity protection. It also prevents the identity leakage that is identity privacy. Identity privacy means when the user wants to share something with another user then he does not require his identity like email, mobile etc. A combination of data indexing technique (Hashing algorithms) along with identity-based encryption algorithm (ABE) [1] is used for this reason. This gives secure optimization of data in the cloud and provides security to users accessing the same data. Attribute-Based-Encryption is an encryption technique which used to encrypt data by using attributes and keys by using any standard algorithms.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

II. LITERATURE SURVEY

User So many survey papers referred to related works. So many works are done on data privacy and data deduplication.

A. Security

For protecting data in cloud Identity-Based Encryption (IBE) [2] was first introduced by Shamir [2], this method used for encryption and decryption based on identity. In this message is encrypted with an identity and a key. The receiver can only read if he match the identity and has the key. It is based on a public key cryptography. Instead of generating a random pair of keys user chose some identity like name and address, or any combination of name, address, telephone number etc. Another algorithm, Fuzzy Identity-Based Encryption [3] was proposed. In this encryption scheme, for encryption, use identity as set of descriptive attributes and for decryption, decrypter's identity and ciphertext has some relation as overlaps. After that, Key-Policy like Attribute-Based Encryption (KP-ABE) [4] and Cipher text-Policy Attribute-Based Encryption (CP-ABE) [5] was proposed. Both are tree based Attribute-Based Encryption schemes. In the KP-ABE [4], ciphertexts are labeled with set of attributes, and identity of user describes in access tree which is associated with private key. In which, decryption is possible when the access tree associated with private key is satisfied by the attributes in the ciphertext. The problem and overhead occur in KP-ABE is resolved by Cipher text-Policy Attribute-Based Encryption (CP-ABE) [5]. In CP-ABE [5], it is just opposite of KP-ABE, in which ciphertexts are labeled with an access structure, due to this encryptor has control over encryption policy, and private keys are provided by attributes of user. In which, decryption is possible if private key associated with attributes satisfied the access tree associated with ciphertext. Due to this, the person who encrypted has authority for encryption policy that why solves the problem and overhead occur in KP-ABE. A multi-authority Attribute-Based Encryption [6] was also proposed. In which, the scheme allows multiple independent authority check attributes and distributes secret keys. In this encryption scheme user can only decrypt if he has authority of attributes. After that more attribute-based encryption schemes with multiple authorities have been proposed [7]-[8], but they are only the same topic based as either a threshold-based Attribute-Based Encryption [7], or have a central authority based encryption [8]. The threshold based ABE has some disadvantages like it is not support collusion attack of many users [7]. The system proposed by Lewko [9] and Muller [10] which is called CP-ABE is most similar to ours like they also decentralize the central authority in multiple ones. But their system not support the attack with attributes authorities, and also many existing system not supported, but our system can support.

B. Data Deduplication

Few works on data deduplication are also proposed in past. So many researchers proposed secure data deduplication methods. One of which was proposed by Yuan et al. [14] for reducing the storage size. It was deduplication system for integrity. System Architecture storage size of the tags. This is also done for ensuring the security and confidentiality to the data.

The perception of Proofs of Ownership (PoW) for deduplication systems proposed by Halevi et al. [13] helps the cloud customers to efficiently prove themselves of owning a file without actually uploading the file itself. This PoW conviction based on the Merkle-Hash Tree are used in several works [13], one of which is proposed for client-side deduplication.

The concept of twin clouds is used for the secure outsourcing of data. Bugiel et al. [11], have provided an architecture consisting of twin clouds. The hybrid cloud techniques are presented by Zhang et al. [12] for supporting the privacy oriented data-intensive computing..

III. PROPOSED SYSTEM

We propose Attribute-based encryption with identity protection for cloud storage. Also, cloud with deduplication, in which the data loaded is first scanned by our master data inspector system which will decide how data should be treated in the cloud system.

ABE algorithm

This is an encryption technique used for sharing encrypted file among multiple users on the basis of attributes assigned to them.

The algorithm works in four steps.

- Setup (λ, U) –> (PK, MK)

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

In this step of the algorithm, the Setup function takes two inputs and produce two keys. It takes λ as a unique identifier of user and universal set U. On basis of λ it determines the attributes from universal attribute set U. Than it generate two keys which are PK (Public Key) and MK (Master Key)

PK generated in this step is used for encrypting the file in next step of the algorithm. The MK generated is stored and it help in generating private key (SK) later on KeyGen function.

- Encrypt (PK, M, S) –> CT

This function takes three inputs which are PK, Message M and user define attribute set S. The S is set of attributes, which give access to all user belongs to attributes of S.

- KeyGen (MK, A) –> SK.

The KeyGen function takes the master key as input and user attribute set 'A'. Here 'A' belong to the user who wants to access the data. This A is matched with S. Than SK which is private key is generated for decryption.

- Decrypt (SK, CT) –> M.

With the help of SK, the ciphertext is decrypted.

RSA Algorithm

The ABE algorithm required the symmetric key algorithm to encrypt and decrypt large files. We are using AES algorithm for encrypting and decrypting the files. RSA is used as a third layer security on top of AES. With the help of ABE, we generate RSA key pairs and use them throughout the algorithm. RSA key pair uses to encrypt and decrypt the AES key.

AES Algorithm

AES algorithm is used for encrypting and decrypting the files before uploading and downloading from the cloud. Before AES algorithm, the AES key needs to decrypt using RSA public-private key pair algorithm. The location of encrypted AES key can be retrieved by Master key generated during setup function of ABE algorithm.

Hashing Algorithms

Data duplication is handled with the help of an SHA256 hash algorithm. The unique file index is created on the indexed database server using unique 64-bit hash key.

The user identities are also stored in hash key form. This help to secure identity of users. The user attributes will be accessed to 64-bit unique hash code.

Framework

Our Proposed system is contains three main modules.

1. ***Server Module:*** All requests first go to this module. This module takes request from a client and communicates with other modules to provide the correct response. Server module consists of one application unit which handles uploading and downloading of a file from cloud storage. This unit also handles the ABE algorithm.
2. ***Master Data Scanner:*** When a file upload request came with server module. It first passes the request to Master Data Scanner. If the file is already present in the cloud then it will not be uploaded twice. The user's ownership of a file will be handling by this module. The even identity of the file for a particular user will be private and will not be changed for any upload.
3. ***Key Generator:*** This Module will provide all types of Key needed to encrypt and decrypt any file. The Key Generator will have all policy stored. It will search in its database and provide the correct key to the correct owner. Also in the case of ABE, Key Generator will generate keys from a different set of the attribute.

So, all these three modules will help to provide a secure and optimized cloud storage solution to our users.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

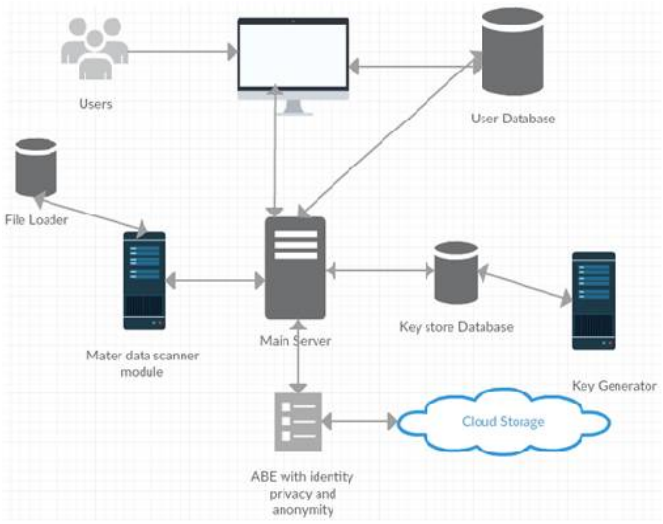

Fig1. Overview of proposed system

IV. MATHEMATICAL MODEL

Let 'S' is the System
S = {s, e, I, O, F, DD, NDD, SS, FS}

Where,
s = start state of the system
e= end state of system
I= Inputs (I) for the System 'S'
O= Output of system
F = Functions used
DD= Deterministic data
NDD= Non-Deterministic Data
SS= Success state
FS= Failure state

Details Explanations:

s: it is defined as start state of the system when the user provides input to the system as file/ data. Input is also as attributes and keys.

e: end state of the system when data is uploaded into the cloud. Also, when data get downloaded from cloud to the local system.

I= {λ, G,U, F, S, A, RD, PubKey, PvtKey} where

λ = security parameter provided by the data owner
G=collection of all identity or attributes
U=universe description (collection of all identity or attributes)
F=File uploaded or download by users
S=Set of attribute provided by user
A=Set of identity provided by receiver
SymKey (AES)= Required for AES Algorithm
PubKey (RSA)=Required for RSA 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)

Vol. 4, Issue 5, May 2016

PvtKey (RSA)=Required for RSA Algorithm

Output (O) is set to outputs System 'S' can provide
O= {PK, MK, CT, SK, M ,T}
PK=public key generated by ABE algorithm
MK=Master Key generated by ABE algorithm and using user secret and access tree (T)
CT=encrypted file or cipher text
The sk=private key generated by Key Generator.
M=Decrypted File
T=Access Tree

DD= It's the file or data uploaded by the user. All data which is already uploaded are deterministic data for our system. Also, the keys are deterministic data for our system.

NDD= All attributes provided by the users.

Success State: When data loaded into cloud or data downloaded from the cloud.

Failure state: When a file fails to upload or download.

V. EXPERIMENTAL SETUP

The setup is done using three machines. One machine work as a client machine. The second one is working as the server where web server and the database server is running. The third computer is for a demonstration of cloud interface, which is a drop box in our scenario.All machine should equip with a wire and connected to the internet.

A. *Dropbox as a cloud storage*

To demonstrate the live scenario of cloud storage we used Dropbox as our cloud server. Below image shows graphical interface of the application interface.

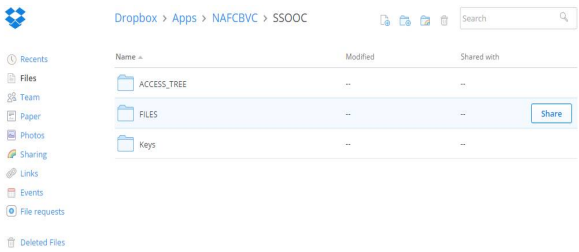

Fig 2: Graphical Interface of Dropbox API.

B.Client Machine

This is where the client will access our system. The client will not access Dropbox UI directly. He will encounter with our client GUI which will give them various options including upload download, delete and update file. The user can also select attribute and share his files.
The Following screen in Figure 3 shows Home page of login user. Login user may upload the file on storage space or downloaded file from storage space.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

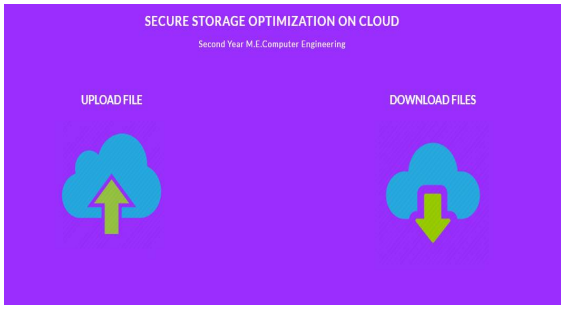

Fig 3: User Home Page

The Following screen in Figure 4 shows the List of filesthat uploaded by users.

Fig 4: User Interface of System

C. Server

This is our system. This is where web server and indexer will be installed. A local MySQL database will be work as an indexer. All algorithms and application modules will run on this machine. This machine will generate keys and store those in Dropbox cloud. Below Fig 4 show keys in Dropbox cloud.

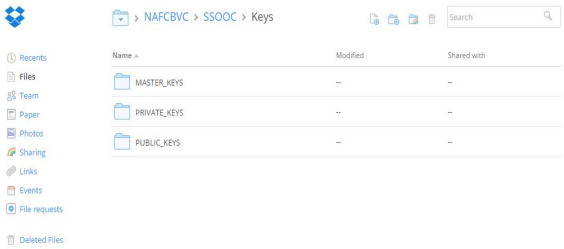

Fig 5: Keys in Cloud Server

V. RESULT AND EXPERIMENT

In For Results and experimental setup the complete working modules need to be implemented. At present status of the project, we are able to do an experiment on downloading and uploading files on the cloud using normal process i.e. without using any encryption and duplication check. We also repeat the same process by applying the deduplication check and encrypting the files using normal algorithms.We found some positive results for our system. The first graph Fig 5 is explaining the behavior of system on uploading and downloading data. The graph is plotted with the size of data and time.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

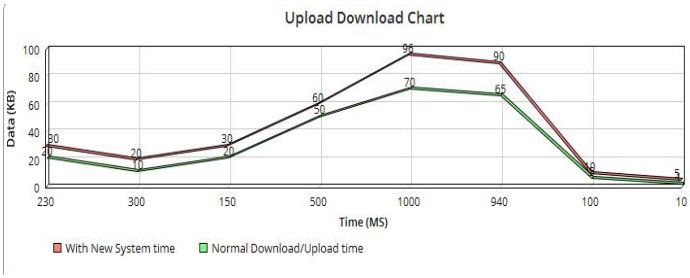

Fig 6: Graph between Data and Download/upload time

The second Result is for data used for a certain amount of request. We noted the data size after a certain number of requests (upload and download) these data sizes are in MB. We again tested with both systems. This test was for checking the effect of deduplication algorithm. Shown in figure 6.

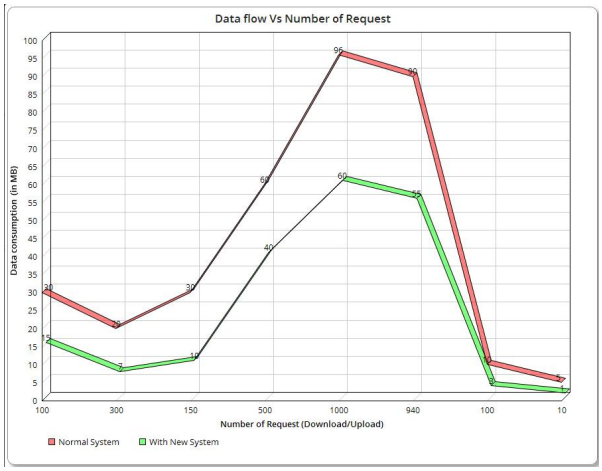

Fig 7: Data VS number of Requests

From above two experiments and results, we can say that our proposed system will work effectively after successful implementation.

ACKNOWLEDGMENT

With immense pleasure, I am presenting this paper on "ACCESS PRIVILEGE CONTROL AND STORAGE OPTIMIZATION USING ATTRIBUTE BASED ENCRYPTION IN CLOUD" as a part of the curriculum of M.E. Computer Engineering at RAJARSHI SHAHU SCHOOL OF ENGINEERING RESEARCH, NARHE, and PUNE. It gives me the proud privilege to complete this paperwork under the valuable guidance of Prof. Dr. S. B. Sonkamble. I thank all the anonymous reviewers and editors for their valuable comments and suggestions to improve the quality of this manuscript..

REFERENCES

1. Taeho Jung, Xiang-Yang Li, Senior Member, IEEE, Zhiguo Wan, and Meng Wan, Member, IEEE "Control Cloud Data Access Privilege And Anonymity With Fully Anonymous Attribute – Based Encryption" IEEE. Jan 2015
2. A. Shamir, Department of Applied Mathematics "Identity-Based cryptosystems and signature schemes," Springer- Verlag, 1985.
3. Sahai and B. Waters, University of California "Fuzzy identity-based encryption," Springer- Verlag 2005
4. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," CCS, 2006.
5. J. Bethencourt, A. Sahai, and B. Waters, Cipher text-policy attribute-based encryption," IEEE SP, May 2007.
6. M. Chase, "Multi-authority attribute based Encryption" Berlin, Germany: Springer - Verlag, 2007,

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

7. Lin, Z. Cao, X. Liang, and J. Shao, Department Of Computer Science and Engineering, Shanghai Jiao Tong University, China "Secure threshold multi-authority attribute based encryption without a central authority," Elsevier Inc, 2010.
8. Božovi´c, D. Soucek, R. Steinwandt, and V. I. Villanyi, "Multi-authority attribute based Encryption with honest-but- curious central Authority," 2012
9. A. Lewko and B. Waters, University of Texas-Austin, "Decentralizing attribute-based Encryption", in Cryptology. Berlin, Springer-Verlag, 2011.
10. S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute- based encryption," Math. Soc., 2009.
11. S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Win clouds: An architecture for secure cloud computing. In Workshop on Cryptography and Security in Clouds (WCSC 2011), 2011.
12. K. Zhang, X. Zhou, Y. Chen, X.Wang, and Y. Ruan. Sonic: privacy aware data-intensive computing on hybrid clouds. In Proceedings of the 18th ACM conference on Computer and communications security, CCS11, ACM, pages 515526, New York, NY, USA, 2011.
13. S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote storage systems. In Y. Chen, G. Danezis, and V. Shmatikov, editors, ACM Conference on Computer and Communications Security, pages 491500. ACM, 2011.
14. J. Yuan and S. Yu. Secure and constant cost public cloud storage auditing with deduplication. IACR Cryptology ePrint Archive, 2013:149, 2013.