ISSN: 2321-8169
67 – 71

A Review: Data Security in Cloud via Decentralized Access Control Technique

Ashwini .S. Kale
Dept of CSE
MGI-COET,Shegaon
mone.ashwini@gmail.com

Niraj N. Kasliwal
Dept of CSE
MGI-COET,Shegaon
kasliwaln@gmail.com

Deepika A. Kadale
Dept of CSE
MGI-COET,Shegaon
deepikakadale@gmail.com

Vaibhav P. Sawalkar
Dept of CSE
MGI-COET,Shegaon
vpsawalkar10@gmail.com

Abstract— Security has been a major issue in data storage. It is a most challenging task to secure the data in cloud infrastructure because most of the data is located in different places. Data security and privacy protection are the two main issues about cloud technology. This paper introduces a review of the data security in cloud via decentralized access control technique. The cloud verifies the authenticity of the user without knowing the user's identity before storing the data. Only valid users can able to decrypt the stored information. Here the term decentralized indicates that key distribution is done in a decentralized way. This decentralized access control scheme grants different access control policies to user to do the operations like creation, modification, and reading the data stored in the cloud. It prevents from the replay attack and secures the data storage in cloud.

Keywords*-Cloud Storage,Data Security,Aceess Control*

*****

I. Introduction

Now a days, cloud storage becomes a most fabulous storage system. Cloud storage is remotely maintained, managed and backed up data on storage system. It acts as a Service and is available to users over a network, which is usually the internet. The service allows the user to store files online and can access them from any location via the internet. The popular cloud storage options are Dropbox, Google Drive, and Microsoft Sky Drive. There are many advantages of Cloud Storage as-

Usability --allows users to drag and drop files between the cloud storage and their local storage.

Accessibility--Stored files can be accessed from anywhere via Internet connection.

Disaster Recovery--Every business have an emergency backup plan ready in the case of an emergency. Cloud storage can be used as a backup plan by businesses by providing a second copy of important files [1]. These files are stored at a remote location and can be accessed through an internet connection.

Cost Savings–Businesses and organizations can often reduce annual operating costs by using cloud storage[2].

As the cloud storage supports to maintain the data remotely, there are high chances of data loss, data stolen or data altered. In simple terms, data security is the practice of keeping data protected from corruption and unauthorized access [3]. The focus behind data security is to ensure privacy while protecting personal or corporate data [3]. Data security is an essential aspect of IT for organizations of every size and type [4]. One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted[5]. In this paper we have review a scheme decentralized access control to secure data in cloud. The cloud verifies the authenticity of the user without knowing the user's identity before storing the data. Only valid users can able to decrypt the stored information. Here the term decentralized indicates that key distribution is done in a decentralized way.

Second section presents the work done by many researchers to secure the data on cloud. It gives the multiple techniques for access control which are carried out for data security on Cloud. Third section provides the details about decentralized access control technique. How the data is stored and access, how the access policies are assigned are mentioned in this section. In fourth section the Attribute based Encryption algorithm is mentioned. The system architecture is explained along with the figure in section fifth. Sixth section provides how the security of protocols implemented in decentralized access control.

II. LITERATURE SURVEY

For cloud based infrastructure, data is located in different places even in the entire globe. Thus, the data security becomes a serious challenge about cloud technology. "Insecure Interfaces and API's", "Data Loss & Leakage", and "Hardware Failure" are the three top most threats in cloud according to the Cloud Security Alliance. Security and privacy protection in clouds are being explored by many researchers [6]. Sultan Aldossary and William Allen discuss on various issues and solutions on data security, privacy availability and integrity in cloud computing [7].Newly, Wang et al. addressed secure and dependable cloud storage. He introduces a flexible distributed storage integrity auditing mechanism, utilizing the hemimorphic token and distributed erasure coded data.

A huge amount of information is being stored in the cloud, and much of this is sensitive information. Access to this sensitive information is the most difficult task in cloud. Only the authorized users have access to valid service. Bibin K Onankunju introduced the different access control techniques used in cloud[8]. In general there are three types of access control: User Based Access Control (UBAC), Role Based Access Control (RBAC), and Attribute Based Access Control (ABAC) [9]. In UBAC, the access control list (ACL) contains the list of users who are authorized to access data[10]. This is not feasible in clouds where there are many users. With role-based access control, access decisions are based on the roles. As a part of an organization, Users take on assigned roles (such as doctor, nurse, teller, manager). The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization [11]. Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role [12]. Varsha D. Mali and Prof.Pramod Patil provide the detailed information about Authentication and Access Control for Cloud Computing Using role based access control mechanism [13]. ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data. There has been some work on ABAC in clouds. All these work use a cryptographic primitive known as Attribute Based Encryption (ABE). The records are encrypted and stored securely in cloud on the basis of ABE under some access policy. Every user has assigned a set of attributes and corresponding keys. When the users have matching set of attributes, they can decrypt the information stored in the cloud. The concept of attribute-based encryption was first proposed by Amit Sahai and Brent Waters [14]. Again ABE has classified in Key Policy Attribute Based Encryption and Ciphertext policy attribute based encryption. Many researchers compare these two techniques. The detailed overview of an attribute Based Encryption Techniques in Cloud Computing Security is presented by Anup R. Nimje, V. T. Gaikwad, Prof. H. N. Datir [15].The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of mono-tonic attributes to control user's access in the system.

Key Policy Attribute Based Encryption (KP-ABE) is the modified form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. To reflect the access tree Structure the secret key of the user is defined. Cipher texts are labeled with sets of attributes and private keys are associated with monotonic access structures that control which cipher texts a user is able to decrypt. Key Policy Attribute Based En-cryption (KP-ABE) scheme is designed for one-to-many communications. Another modified form of ABE called CP-ABE introduced by Sahai. In a CP-ABE scheme, every cipher text is associated with an access policy on attributes, and every user's private key is associated with a set of attributes [16]. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. CP-ABE works in the reverse way of KP-ABE. The access structure of this scheme or algorithm, it inherits the same method which was used in KP-ABE to build. And the access structure built in the encrypted data can let the encrypted data choose which key can recover the data; it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is similar to the traditional access control schemes[17]. The encrypt or who specifies the threshold access structure for his interested attributes while encrypting a message. Based on this access structure message is then encrypted such that only those whose attributes satisfy the access structure can decrypt it. The most existing ABE schemes are derived from the CP- ABE scheme. V Bozovic, D Socek, R Steinwandt, and Vil-lanyi, introduce Multi-authority attribute-based encryption. In this scheme it use multiple parties to distribute attributes for users. A Multi-Authority ABE system is composed of K attribute authorities and one central authority. Each attribute authority is also assigned a value dk.[18].

All the above mentioned schemes for access control of data stored in cloud use the centralized approach. That means only one KDC is responsible for distribution of key for accessing data stored on cloud. But in reality there is huge number of cloud user who wants to perform the operations on data stored in cloud. Thus, only one KDC acts as a single point of failure and unable to handle a large crowd of users on cloud. To overcome drawback of single KDC we go for the Decentralized Access Control Technique. In this scheme cloud verifies the authenticity of the user without knowing the user's identity before storing the data. Only valid users can able to decrypt the stored information. Here the term decentralized indicates that key distribution is done in a decentralized way.

III. DECENTRALIZED ACEES CONTROL SCHEME

In earlier systems, only the creator of data can manipulate the data but other users can only read the data. Write access is not permitted other than the creator of the data. In decentralized system, any valid user can access the data stored on cloud and edit the same data. The architecture of cloud secure storage by using decentralized access control technique is shown in Fig.1

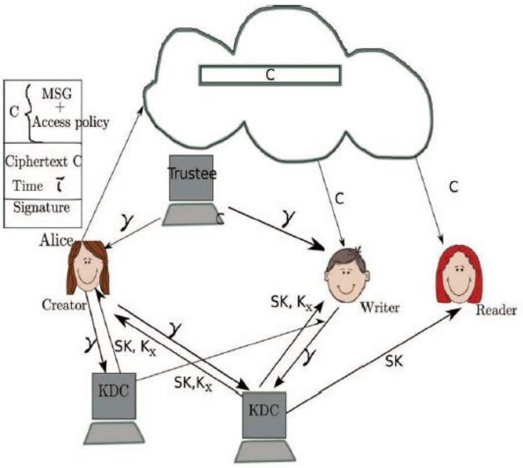

Figure1. Decentralized Access Control

In figure there are three users for cloud namely Creator (Alice), Writer and Reader. A trustee can be someone like the federal government who manages social insurance numbers etc. who is assumed to be honest. Creator (Alice) receives the token 'γ' from trustee to operate with the cloud. The same token 'γ' is presented to different KDC systems. KDC now responsible to give secrete key (SK) for encryption and decryption of data stored on cloud. Kx (keys for signing) is also provided by KDC to Creator (Alice) to sign the data before storing on the cloud. Creator (Alice) encrypts the message under the access policy X. The access policy decides who can access the data stored in the cloud. The Creator (Alice) defines a claim policy Y to prove the authenticity and signs of the message under this claim. The cipher text C with a signature c is sent to the cloud. The cloud verifies the signature and stores the cipher text C.

When a reader wants to read the message in the cloud, KDC sends the same SK for decryption of data but the user has attributes matching with the access policy attached with message can only decrypt the data and able to get original data.

Write operation is also proceeds in similar way as creation of data. The key is provided by KDC to Writer to decrypt the data. Data is decrypted only when the User has matching attributes defined by Creator (Alice) in access policy. If the matching attributes are there, Writer can edit the data stored on cloud and again define the access policy for the same by signing the edited message.

A. *Data storage in Cloud*

A user first registers itself with one or more trustees. For simplicity we assume there is one trustee. The trustee gives it a token γ. The user on presenting this token obtains attributes and secret keys from one or more KDCs. The user also receives secret keys SK for encrypting messages. The user then creates an access policy X which is a monotone Boolean function. The message is then encrypted under the access policy as-

$$C = ABE.Encrypt(MSG,X)$$

B. *Reading from the cloud*

When a user requests data from the cloud, the cloud sends the ciphertext C using SSH protocol[19]. Decryption proceeds using algorithm ABE.

C. *Writing to the cloud*

To write to an already existing file, the user must send its message with the claim policy as done during file creation. The cloud verifies the claim policy, and only if the user is authentic, is allowed to write on the file [20].

IV. ATTRIBUTE BASED ENCRYPTION

Assumptions for the decentralized access control technique are as-

1) The cloud is honest-but-curious, which means that the cloud administrators can be interested in viewing user's content, but cannot modify it.

2) Users can have either read or write or both accesses to a file stored in the cloud.

3) All communications between users/clouds are secured by Secure Shell Protocol, SSH.

The backbone of decentralized access control scheme is Attribute based encryption algorithm. The ABE algorithm is well explained in [21] and is as follows:

Input: set of attribute {a1, a2, an}
Message M
User Identity token T
Access policies X
Output: Encrypted document C
Signed Document σ
Key K
Encrypted document M

Processing:

Step:1 Initialization

g is generator of cyclic group G

Random numbers α i, yi$\in$Zq

Step:2 Key generation

Secret key SK and public key PK:

SK = { α i, yi, i $\in$Lj}.

PK = {e (g, g) α i, gyi, i $\in$Lj}.

Step:3 Encrypted documents

C = ABE. Encrypt (M, X, SK[i])

σ = ABS. Sign (PK, T, MSG, X)

Step:4 Decrypt Message using

M= ABE. Decrypt(C, {SK, T})

V. System Architecture

The figure 2 represents the architecture of the access control in cloud storage. There are five main modules: Trustee, Creator, KDC, User, and Cloud Storage.

1. Trustee: Trustee is assumed to be honest. When the Creator wants to store the data on cloud he first registers the details to Trustee. On submitting the details, Trustee is responsible to give the token to Creator.

2. Creator: User who want to upload the file on Cloud is referred as Creator.

3. KDC: Key Distribution Center provides the keys needed for encryption and decryption. Also provides the keys for Signing and verification purpose.

4. User: User may be the creator/Reader or may acts as Writer to modify the content of data stored on cloud.

5. Cloud Storage: Responsible to save the documents and manage the files among different users.

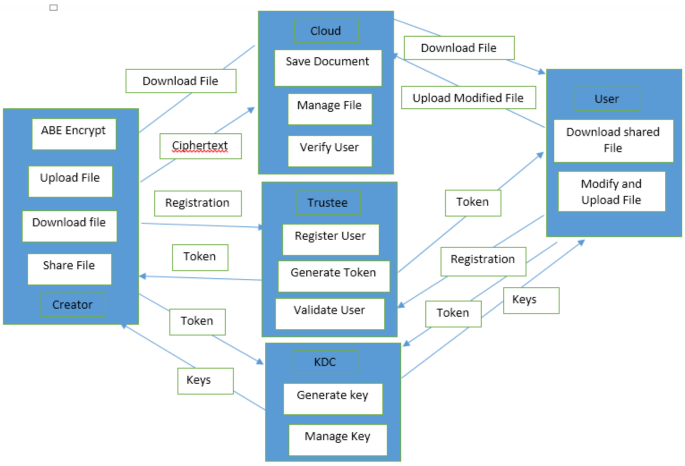

Figure 2. System Architecture of Access Control in Cloud

A.Upload a data on Cloud:

Following operations are carried out to upload a data on Cloud-

1.First User register with Trustee. He/she gives his/her personal information to Trustee. On the basis of this information, Trustee provides the token T for User.

2.After receiving the token from Trustee, Creator sends the same token to one or more KDC. For simplicity, we assume only one KDC.

3.Now KDC provides the four keys to Creator, PK, SK [for encryption/decryption] & ASK, APK for signing/verifying and KDC token KT.

4.By using previously seen Attribute Based Encryption algorithm, User encrypt the message as:

C=ABE. Encrypt (MSG,SK)

5.After encrypting the message, User generates the authentication policy and access policy(X) for the same.User signs the message σ = ABS. Sign (PK, T, MSG, X) and sent the file to Cloud.

6. The following information is then sent to the cloud

c = (C, T, σ, P).

7.At Cloud end, after receiving the data, Cloud verifies the access claim using the algorithm ABS Verify. The creator checks the value of V = ABS.Verify(T, σ, C, P). If V = 0, then authentication has failed and the message is discarded. Else, the message (C, P) is stored in the cloud.

B.Download files from Cloud

1. When User wants to download the data from Cloud first he goes under the Verification process. Verification of user is done as per the above process.

2. If Authentication is done by User successfully, User requests data from the cloud.

3. Using SSH protocol and after matching access permission X,Cloud sends the cipher text C to User.

4. Algorithm ABE, Decrypt(C, SK) is used to decrypt the data and the original message MSG is delivered to User.

VI. SECURITY OF THE PROTOCOL

The section proves the security of the protocol. User who wants to write a file to the cloud first authenticated. Cloud validates the access claim of User. If the validation is successfully done then User can write to cloud. An invalid user cannot receive attributes from a KDC, if it does not have the credentials from the trustee. If a user's credentials are revoked, then it cannot replace data with previous stale data, thus preventing replay attacks[22].

VII. Conclusion

This paper represents a review of Data Security in Cloud via Decentralized Access Control Technique. The scheme provides secure cloud storage. File which are stored on cloud are associated with file access policies. These access policies are used whenever there is read write request for file.

Uploading and downloading of a file to a cloud with standard Encryption or Decryption. It is a Decentralized access of system in which key distribution is done in a decentralized way. By use of multiple KDCs, we overcome the drawbacks of single KDC to handle the large crowed on cloud and single point of failure. Decentralized Access Control guarantees the data security in cloud.

REFERENCES

[1] http://aptrongwalior.blogspot.in

[2] Baiju NT, “advantages and disadvantages of Cloud Storage”, 28th Jul `14

[3] http://www.spamlaws.com/data-security.html

[4] https://medium.com/@PritishCh/digital-data-security-cdadb95c191b

[5] https://www.techopedia.com/definition/26464/data-security

[6] Hemalatha, V. Balaji, “Anonymous Authentication for Decentralized Access Control of Cloud data”, International Journal of Advance Research in Computer Science & Studies, Volume 2, Issue 11, November 2014

[7] Sultan Aldossary, William Allen, “ Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions”, nternational Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.

[8] Shraddha V. Mokle , Nuzhat F. Shaikh , “Decentralized Access Control Schemes for Data Storage on Cloud”, Creative Commons Attribution International License

[9] “An Introduction To Role-based Access Control”, NIST/ITL Bulletin, December,1995

[10] Swati P. Ramteke, Priya S. Karemore, S.S. Golai, “Intrusion Detection of Masquerading Attacks & Secure Authentication in Cloud ”, IOSR Journal of Computer Engineering, Volume 9, Issue 2 ,Jan. - Feb. 2013

[11] https://cs.stanford.edu/people/eroberts/cs181/projects/computer-crime/prevent.html

[12] Varsha D. Mali1, Prof.Pramod Patil, “ Authentication and Access Control for Cloud Computing Using RBDAC Mechanism”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 11, November 2016

[13] John Bethencourt, Amit Sahai, Brent Waters “Ciphertext-Policy Attribute-Based Encryption”, IEEE Symposium on Security and Privacy(SP'07)

[14] Mr. Anup R. Nimje, Prof. V. T. Gaikwad ,Prof. H. N. Datir, “Attribute -Based Encryption Techniques in Cloud Computing Security : An Overview”, International Journal of Computer Trends and Technology, volume4 , Issue3- 2013

[15] “Attribute-Based Encryption Techniques in Cloud”

[16] RajaniKanth Aluvalu ,Lakshmi Muddana, “A Survey on Access Control Models in Cloud Computing”, Springer International Publishing Switzerland 2015

[17] P.Madhubala1 , Dr.P.Thangaraj, “Comprehensive and Comparative Analysis of Cryptographic Solutions in Cloud”, International Journal of Innovative Research in Computer and Communication Engineering, ISSN ONLINE(2320-9801)

[18] RajaniKanth Aluvalu1 and Lakshmi Muddana, “A Survey on Access Control Models in Cloud Computing” , Conference on Emerging ICT for Bridging the Future, December 2014

[19] Ms. P.Ranjima, Ms. Sumathi. D, Ms.Minimol Mathew, Ms.Anisha Viswan, “Attribute Based Encryption with Privacy Preserving and User Revocation in Cloud”, JETIR, March 2015, Volume 2, Issue 3

[20] R.Vaishali , M.Menaka, “Attribute based Encryption and Key
Distribution for Secure Storage in Clouds”, IJEDR Conference Proceeding (NCISECT 2015) | ISSN: 2321 -9939

[21] RajaniKanth Aluvalu1 and Lakshmi Muddana, “A Survey on Access Control Models in Cloud Computing” , Conference on Emerging ICT for Bridging the Future, December 2014

[22] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, “Decentralized Access Control with Annonymous Authentication of Data Stored in Cloud”, IEEE Transactions on Parallel and Distributed Computing, 2014 ,volume 25