IJCAT - International Journal of Computing and Technology, Volume 3, Issue 4, April 2016
ISSN : 2348 - 6090
www.IJCAT.org

Secure Data Sharing Encryption Schemes in Cloud Storage: A Review

[1] Shraddha Deshmukh, [2] Prutha Sontakke, [3] Mithil Wasnik

[1,2,3] Department of Computer Technology, Nagpur University,
Rajiv Gandhi College of Engineering and Research, Nagpur, Maharashtra, India

Abstract - A model based on cloud computing wherein data is being accessed from the cloud and through the internet without any direct affiliation to the server. The services of cloud can be accessed as long as the internet service is accessed. In this paper, survey on many schemes like Key-Policy Attribute-Based coding, Cipher text- Policy Attribute-Based coding, Cipher text Policy Attribute Set primarily based coding, Fuzzy Identity-Based coding, gradable Identity-Based coding, gradable Attribute-Based Encryption and gradable Attribute-Set-Based Encryption for access management of outsourced information are mentioned.

Keywords **- Cloud Computing, Data Confidentiality, Fine-Grained Access Control.**

1. Introduction

The inspiration of cloud computing characterizes the cloud computing different form that of the ancient hosting. A cloud is non-public or public. In public, cloud service is oversubscribed to anyone on the net. (Currently, Amazon net Services are that the largest public cloud supplier.) Privately, cloud act as a proprietary network or hosted services area unit equipped to limited folks through information Centre. Dynamic access of cloud is of great importance to the computing resources and IT services. Cloud computing offers vital innovations in virtualization and distributed computing, improves access to high-speed net. It serves as the commodity for weak economy by the high speed access to it. The different service models of cloud are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and computer code as a Service (Saas).

The protection measures needed to be taken during accessing its resources are:

1.1 Privacy

All of the activities carried out by the client should not be by any means be the source for the interception of the data. Not only the data but the user or client log of the activities needs to be maintained along with digital credentials.

1.2 Access Control

The individuality and the role of each individual need to be specified who has access to what kind of data needs to be defined by the service provider. Several techniques were known for implementing fine grained access control. [11]

1.3 Data Confidentiality

The term data confidentiality refers to the fact that the data of the third party is not compromised on any condition to the outsider or the intruder which should be ensured by the service provider. [8][10]

1.4 Data security

Security is the foremost prerequisites for the customer and is chief factor for the provider as well. No collusion or any type of attack should not tamper the customer's data. [9]

The effective implementation for the above mentioned security issues would be encrypting data by using certain encryption techniques, which allowed flexibility in specifying differential access rights of individual users in a feasible way.

2. Study on Cloud Storage Schemes

2.1 Attribute Based Encryption using Cipher Text Policy

The person who encrypted the data designed the access policy to determine the person responsible for data decryption. This system was similar to Role Based Access

Control (RBAC). There was a chance for collusion attack if the attributes describing the cipher-text was combined. Private Key randomization technique was used to generate keys in CP-ABE. Instead of KP-ABE which denoted cipher text, CP-ABE inverse of KP-ABE as a substitute while access policies were built based on the user's keys. But it was limited to the fact that encryptor were not allowed to create the access policies which urged for development of CP-ABE [2]. The key provider was responsible for granting the keys and creating access policies. Altogether, the entire KP-ABE system was influenced by trust. CP-ABE was used to recognize the complex access control in cipher-texts even in case of untrusted servers. This system included the attributes that denoted the user credentials. CP-ABE was found to be more efficient than KP-ABE.

2.2 Attribute-Based Encryption in Hierarchical Manner

HABE was a new approach which blended HIBE and CP-ABE can be created for efficient sharing of confidential data on the cloud server. This was followed by application of PRE and LRE to HABE scheme for the revocation process. This HABE scheme was expected to attain complete delegation, scalability, fine-grained access control and high performance. This system contained the advantages and disadvantages of HIBE and CP-ABE.

2.3 Attribute Based Encryption in Medical Data Exchange

To make the data exchange secure in cloud, a system was proposed that granted fine grained access control to the outsourced data by combining KP- ABE, PRE and LRE [9]. The purpose of the system was to provide secure access control for medical data exchange and secure key management. This scheme greatly reduced the data owner's difficulties by delegating it to the cloud servers. A medical data exchange scenario had been taken into consideration. Here, the patient wanted to send the files requested by the doctors. Initially, the patient must send the secret key, the PRE key and the URL of the cloud storage to the doctor via email. Then, the patient needed to upload the encrypted files (i.e., files are encrypted using the Data Encryption Key, DEK) and the encrypted DEK (i.e., DEK is encrypted using KP-ABE whose access structure is satisfied by the secret key sent to the doctor) to the cloud storage. The doctor requests and receives both encrypted files and encrypted DEK. After receiving the response from the cloud, the doctor used his secret key to decrypt the encrypted DEK. Then, the original DEK was used to decrypt the encrypted files. The cloud storage server was assumed to be semi trusted.

2.4 Attribute Based Encryption in Personal Health Records

A centralized storage system with hierarchies was developed for sharing the PHR [13]. PHR was outsourced on the cloud service provider. Building PHR in the form of distributed storage stimulates the key management overhead. Central Authority (CA) could provide solutions to this problem. It was not good to believe a CA for handling the storage which guided to key escrow problem. To treat this problem, users in the system were classified as personal and public domains. Personal domain dealt with the personal information of the patient which was accessible by the data owner. Public domain comprised of different types of information. An authority was assigned to each type of information. PHR used ABE.

Thus, personal domain was controlled by the Data Owner which used KP-ABE and the public domain was controlled by multiple attribute authorities which used Multiple Authority - Attribute Based Encryption (MAABE).

The attribute authority was responsible for granting and revoking access to the users. The attributes present in the cipher-text were modified to update the access policies. In Break-glass situations, an emergency department was enclosed which granted temporary read keys to the authorized users in the emergency sites. Scalability and Efficiency were improved in this system which allowed secure and scalable sharing of PHRs.

2.5 Enhancing Security by CP-ABE

A scheme which ensured data integrity and security in data outsourcing using CP-ABE was suggested [11] the owner of the data was responsible for defining and enforcing the policies for attributes and not for users. Thus, unauthorized access was effectively blocked. The security model of the cloud storage architecture consists of the Key Generation Centre, Data Storing Centre, Data Owner and the User. The Data Storage Centre and the Key Generation Centre are assumed to be semi-trusted. The attribute sets were identified by private keys. The key issuing protocol involved key generation and data storing centers. This was followed by generation of secret keys using the secure 2PC protocol. Keys are provided to those users who possess the correct attributes. As the key issuing protocol involved two authorities, no one could individually generate the secret keys for the user.

2.6 Temporal Attribute-Based Access Control

Temporal Attribute Based Encryption was designed by adding time slot to the attributes [7]. In order to improve the efficiency of multi-authority cloud storage systems,

CP-ABE is applied in such schemes. Due to the attribute revocation problem, existing CP-ABE schemes are not directly enforced to data access control for storage systems in cloud. The cloud storage system consists of multiple attribute authorities and they are independent of each other. As there were multiple authorities, no central authority was required to manage the entire cloud storage system and it was ensured that the entire security of the cloud storage system was not dependent on the central authority. Temporal Attribute-based Access Control (TAAC) was proposed to provide the efficient data access control schemes in multi authority cloud storage systems on attribute level. In order to improve the efficiency of cloud storage, re-encryption of cipher text could be avoided.

The purpose of TAAC was to provide time slots and associate the time slot with attributes. The attribute authority could revoke or re-grant the user in a particular time slot without the knowledge of other authorities (i.e., users can access the attributes from other authorities, only the attributes from the particular authority is revoked). Any legal user can download the cipher-text from the system and only those who have the attributes are allowed to decrypt the cipher-text which is associated with the access policy and the particular time slot. The algorithms used in TAAC to design the framework are Global Setup, Authority Setup, SKeyGen, UKeyGen, DKeyCom, Encrypt and Decrypt. Symmetric algorithms are used to encrypt the data and TAAC is used to encrypt the content key. The Secret keys were given to those users who possessed the attributes. The Update Keys were then published in the public bulletin boards. Secret keys and Update keys were used to generate decryption key for time slot. The four phases in TAAC were System Initialization, Key Generation by Attribute Authorities, and Data Encryption by owners and Data Decryption by users. TAAC enhanced the scalability and flexibility in constructing an efficient multi authority cloud storage system.

2.7 Attribute Based Encryption using Key Policy

KPABE is proposed to share in the fine grained level. This system involves cipher-texts and private keys. A new encryption scheme namely Attribute Based Encryption (ABE) was discovered in a fine grained manner [1]. ABE consists of four steps namely Setup, Encryption, Key Generation and Decryption. User generates the private key acts like a local key authority. Storing data in the form of cipher-text at the third party storage is essential. The limitation of using encrypted message is that it could be distributed at coarse-grained level only.. Cipher texts are tagged with attributes. Private keys linked with access structures govern the cipher-texts needed for decryption. The authors admit HIBE for assigning private keys. Fine grained access control engages a server for storing data. The security concerns involve insider attackers and a hierarchy which acts as a mediator and decrypts the data for the third party or gives the private decryption key to the third party. These security concerns are solved by encrypting data and allowing users to decrypt as per the security. In Secret Sharing Schemes (SSS), secret is divided and shared among the members. SSS is associated with an access structure that represents a tree. Access trees are constructed using attributes in which the intermediate nodes are the threshold gates and the child nodes are connected with the attributes. By using attribute concepts, private keys are generated and delegated to lower level users. It prevents collusion attacks. Audit log is a complicated application in which encryption makes it more complex. Providing the entire audit log to a single analyst leads to insecurity. By associating attribute based access structures to this audit log, unauthorized access is prevented and collusion by different users is avoided. A broadcast encryption named Targeted Broadcast works well with the help of attributes.

3. Review of Cloud Encryption Schemes

3.1 Re-Encryption in Unsecured Clouds

A re-encryption scheme was advised to increase the data security in untrusted clouds [6]. A cloud environment consists of many cloud servers. The authors need to store encrypted data into the cloud. To avoid the revoked users accessing the data file with their decrypt keys, the contents must be re-encrypted and the new keys were rendered to the empowered users. Four cloud servers namely CS1, CS2, CS3 and CS4 have been considered. The data owner re-encrypts all the old cipher-text using the new re-encryption keys. This can be done by propagated re-encryption commands through the entire network. The revoked users gained the old cipher-text which was decrypted by their old decryption keys if the server is not updated due to network failures.

The independent re-encryption by the cloud servers without obtaining the commands from the data owner (i.e., avert the command driven re-encryption scheme) is the feasible solution to this problem. The access time and access control were associated for data of Reliable re-encryption scheme in unreliable clouds (R3 scheme). The objective to design the R3 scheme was to permit the cloud servers to re-encrypt the data automatically based on the internal clock. This scheme applied ABE and PRE. Initializing the data owner, access for the users to read data and access for the data owner to write data are the three components in R3 scheme. This scheme shows the access

control correctness, data consistency, confidentiality and data efficiency.

3.2 ESC Scheme

A hierarchical organization using cloud storage services has been designed for efficiently sharing the services. The ESC scheme has been suggested for its usage in hierarchical cloud systems [5]. The top level user is the owner of the organization and the employees working under the owner are considered to be the lower level users. The trusted third party was a root-Private Key Generator (root-PKG) who acted as the topmost level to the owner. The root-PKG delegates the owner to provide the secret keys to the lower level users. As the owner granted access to multiple recipients, the system adopted one-to-many encryption and HIBE algorithm.

The hierarchical identity-based architecture consisted of a domain which included the top level user and the lower level user, which were responsible for the authentication and the secret key transmissions. The domain shares the cloud storage services. When the sender wanted to encrypt and store a file, it was sufficient to store a single cipher-text copy on the cloud. The file could be recovered by the owner and the concerned people using private keys. The unauthorized employees inside the domain and the outside attackers were unable to recover the cipher-text. Therefore attacks were avoided by this scheme. The steps carried out in ESC scheme included Root Setup, Dom Setup, One2ManyEnc, User Dec and Recipients Dec. Security and Performance related issues have been given due importance in this scheme.

3.3 Independent Cloud Systems

A business model which consisted of three cloud systems was advised to ensure data confidentiality [8]. The unauthorized insiders in the cloud leak the data. To avoid this, data was stored in one service provider and the encryption or decryption was performed in another service provider. The encryption or decryption system was not aware of the data stored in storage service provider. It was necessary that data must be encrypted first and then stored in storage service provider. The third cloud system was for application systems such as CRM. All the three cloud systems are independent.

3.4 Cloud Storage System Based on Erasure Code

Constructing a secure distributed cloud storage system was a major dispute when it executed multiple functions. Threshold PRE scheme and the decentralized erasure code was suggested for the distributed cloud storage system [10]. The decentralized cloud storage system consisted of two servers namely distributed storage servers and key servers. Maintaining separate servers for different functionalities was important for the data confidentiality because the servers are considered to be semi-trusted. Encoding and forwarding functions was performed by storage servers and partial decryption is performed by key servers. Data forwarding used PRE schemes. The encoding on the encrypted messages and the forwarding procedures were executed on the encrypted and encoded messages was performed by encrypting schemes. System Setup, Data Storage, Data Forwarding, and Data Retrieval were the four phases in distributed storage system. During data forwarding stage User A forwards the message to user B. Initially, user A downloads the stored encrypted message from the cloud and decrypts the cipher-text using his secret keys. This was followed by encryption of the message by user A using user B's public key. The new cipher-text was stored in the cloud for the purpose of forwarding. The cipher-text was then downloaded and then decrypted by user B using secret keys.

M. Various Encryption Schemes various encryption schemes dealing with sharing of outsourced data in a safe manner have been discussed [12]. In KP-ABE, the encryptor creates attributes and encrypts data. The problem dealt with the identification of the person who generated private keys responsible for creating the access policies. In CP-ABE, the user credentials were accepted as attribute, and the encryptor were responsible for creating the access policies. The enhancement of CP-ABE is Cipher text Policy-Attribute Set Based Encryption (CP-ASBE).

In CP-ASBE, the recursive set managed attributes and the users were granted based on the enforcement of the dynamic constraints. The attributes were grouped into sets and the users who possessed attributes from those sets have access only to those particular sets. This leads to increase in accuracy in confidentiality. In Fuzzy Identity Based Encryption, the attributes chosen were identities. The private key is assigned with the identity a, and the cipher text is encrypted using the identity a'. To decrypt, identities a and a' are measured using set overlap distance metric to find the similarity. It permits error tolerance. The hierarchy of HIBE includes Identity Based Encryption system. The private keys were issued by the identities at the top level to its descendants in the lower level. Low level identities are not allowed to decrypt the message.

The Hierarchical Attribute Set Based Encryption (HASBE) was extension of CP-ASBE with hierarchy of users. It was decided that HASBE was the upgraded encryption scheme which shared the secured outsourced data in the cloud service provider by analyzing these algorithms.

4. Conclusion

This paper discusses the cloud storage system and the encryption techniques elaborately. Encryption techniques with makes the storage system more secure and as well as scalable. Implementation of an encryption system on the cloud storage is been done in order to achieve minimum storage and computation cost that provides the necessary impetus for research. Combination of centralized and decentralized storage systems existed in organizations.

References

[1] M. Nelson, "Building an Open Cloud," Science. vol. 34 no. 5935 pp. 1656–1657, June 2009.

[2] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[4] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[5] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.

[6] Yanli Ren and Dawu Gu,"Efficient Hierarchical Identity Based Encryption Scheme in the Standard Model"in Proc. Informatica 32 (2008),pp 207–211.

[7] G.Wang, Q. Liu, and J.Wu, "Hierachical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.

[8] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing"in Proc.IEEE Transactions on Information Forensics and Security, vol.7, No.2, April 2012.

[9] S.G.Shini and K.Chitharanjan, "Secure Cloud based Medical Data exchange using Attribute based Encryption," Special Issue of International Journal of Computer Applications on Advanced Computing and Communication Technologies for HPC Applications – ACCTHPCA, 2012.

[10] Hsiao-Ying Lin and Wen-Guey Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," IEEE Transactions on parallel and distributed systems, Volume 23, No.6, 2012.

[11] B.Raja Sekhar, Sunil Kumar, L.Swathi Reddy and V.PoornaChandar, "CP-ABE Based Encryption for Secured Cloud Storage Acces," International Journal of Scientific & Engineering Research, Volume 3, Issue 9, 2012.

[12] K.Priyadarsini and C.Thirumalai selvan, "A Survey on Encryption Schemes for Data Sharing in Cloud Computing," International Journal of Computer Science and Information Technology & Security (IJCSITS), Volume 2, No.5, 2012.

Author Profile:

Shraddha Deshmukh is currently in the final year of degree course of bachelor of engineering from Rajiv Gandhi College of engineering and Research, Wanadongri, Nagpur under Rashtrasant Tukdoji Maharaj Nagpur University.

Prutha Sontakke is currently in the final year of degree course of bachelor of engineering from Rajiv Gandhi College of engineering and Research, Wanadongri, Nagpur under Rashtrasant Tukdoji Maharaj Nagpur University.

Prof. Mithil Wasnik the guide and lecturer in Rajiv Gandhi College of engineering and Research, Wanadongri, Nagpur under Rashtrasant Tukdoji Maharaj Nagpur University.