A Survey on Cloud Storage Systems and Encryption Schemes

J. Raghavi [#1] & S. Krishna Anand [*2]
Computer Science & Engineering, School of Computing,
SASTRA University, Tirumalaisamudram, Thanjavur-613401,Tamilnadu, India.
[1]raghaviprakash@gmail.com
* Computer Science & Engineering, School of Computing,
SASTRA University, Tirumalaisamudram, Thanjavur-613401,Tamilnadu, India.
[2]skanand86@gmail.com

***Abstract* - Cloud computing is the collection of networked computers sharing the resources on-demand. The increasing use of cloud computing over the globe has brought into focus a need to design a secure cloud storage system. For safe and satisfactory implementation of the same, there is a need to place emphasis on the problems arising in the same. The chief one is the unauthorized access which prevents data confidentiality. A secure cloud storage model guarantees security and robustness. The essential task is to encrypt the data before storing it for security purposes. This paper deals with the uncertainties of using centralized and de-centralized storage systems. It also explains the various encryption techniques used to prevent the information from eavesdropping.**

Keyword-Cloud storage, Centralization, Decentralization, Encryption, Re-encryption

I. INTRODUCTION

Cloud Computing is an interesting and emerging technology which makes the cloud easily accessible to the internet users. Cloud Computing has been used extensively in personal and commercial business applications. Cloud storage is a boon to the enterprise users. Instead of owning the resources which are inaccessible during most of the time, cloud storage provides them pay per use concept. There is a significant reduction in maintenance cost. Besides, data is also made portable. The primary advantage is retrieval of backup of replica files. There is a dire necessity to handle challenges like data leakage, key management and performance. Virtualization is the key concept which influences the cloud computing.

The manner in which information could be stored in the cloud could be either centralized or distributed. The advantage with centralized storage is that it is easy to handle. However, distributed storage is a challenge to the data owner and impractical to implement. Most of the real world systems incorporate a combination of centralized and distributed storage systems. Besides, relying on a third party cloud storage provider could lead to security problems. To assure data confidentiality, data owner stores an encrypted data in the cloud. It is good to use Attribute Based Encryption instead of ordinary encryption techniques.

Key Policy - Attribute Based Encryption (KP-ABE), an encryption scheme was suggested to make the cloud storage more secure [1]. Ciphertext Policy - Attribute Based Encryption (CP-ABE) is designed to overcome the limitations of KP-ABE [2]. An encryption scheme namely Hierarchical Attribute Based Encryption (HABE) scheme is formed by combining Hierarchical Identity Based Encryption (HIBE) and CP-ABE. The advantage of using HABE is the maintenance of confidentiality in data [3]. By aggregating these encryption schemes namely KP-ABE, Proxy Re-encryption (PRE) and Lazy Re-encryption (LRE), the storage system is provided with security, scalability and fine grained access control [4]. Hierarchical Identity – Based Architecture is used for designing Efficient Sharing of Secure Cloud Services (ESC) scheme [5].

Data can also be re-encrypted in unreliable cloud storage [6]. Attribute Based Access Control, an existing technique was altered in multi-authority cloud storage system for security and scalability. This is achieved by creating and associating the time slot along with attributes [7]. A business model scheme was discovered with three independent cloud storage systems to assure data confidentiality [8]. KP-ABE, PRE and LRE were integrated for improving key management functions [9]. An idea of maintaining separate servers for storing data and key adopts encryption and encoding techniques for data confidentiality [10]. CP-ABE scheme and the key issuing protocol are utilized for enhancing the security [11]. A study of diverse encryption schemes is carried out to determine the best encryption scheme [12]. The centralized cloud storage with multiple attribute authorities was suggested for creating Personal Health Records (PHR) [13].

II. STUDY ON CLOUD STORAGE AND ENCRYPTIONS SCHEMES

A. Key Policy-Attribute Based Encryption

A new encryption scheme namely Attribute Based Encryption (ABE) was discovered in a fine grained manner [1]. 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. To overcome this limitation, KP-ABE is proposed to share in the fine grained level. This system involves cipher-texts and private keys. 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. Hierarchy 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. It prevents collusion attacks. ABE consists of four steps namely Setup, Encryption, Key Generation and Decryption. 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. The user, who generates the private key acts like a local key authority. 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.

B. Ciphertext Policy - Attribute Based Encryption

CP-ABE, an alternative to KP-ABE was suggested. The inverse of KP-ABE is CP-ABE. In KP-ABE, attributes denote the cipher-texts while access policies are built based on the user's keys. However, the limitation in KP-ABE system is that encryptors are not allowed to create the access policies. This in turn leads to development of CP-ABE [2]. The key provider is responsible for granting the keys and creating access policies. Altogether, the entire KP-ABE system is influenced by trust. CP-ABE is used to recognize the complex access control in cipher-texts even in case of untrusted servers. This system includes the attributes that denote the user credentials. The person who encrypts the data designs the access policy to determine the person responsible for data decryption. This system is similar to Role Based Access Control (RBAC). Collusion attack is eliminated efficiently by CP-ABE rather than KP-ABE. There is a chance for collusion attack if the attributes describing the cipher-text is combined. Private key randomization technique is used to generate keys in CP-ABE. CP-ABE is found to be more efficient than KP-ABE.

C. Providing Fine Grained Data Access Control

Combining encryption schemes was suggested to provide fine grained data access control [4]. Providing security on untrusted servers is a challenging issue. To increase the level of security, some cryptographic methods are applied to reveal the data decryption keys to the empowered users. Attempting to attain the scalability and the fine grained data access control paves the way for computation overhead by data management and key distribution. A mechanism is proposed by combining KP-ABE, PRE and LRE. This system is utilized to achieve scalability, data confidentiality and fine grainedness. The significant task of the system is to allow the data owner to grant data access control to unauthorized servers without going into the finer details. Access policies are enforced based on the attributes. Access control and the keys of the users are guaranteed with security. Data files use attributes for access structure and KP-ABE is applied to safeguard the data decryption keys for fine grained data access control. Computation overhead is generated during creation of KP-ABE. KP-ABE requires the data owner to be always online during updation. Combining KP-ABE with PRE reduces the overhead since the data owners delegate the files to servers without revealing the original content. Overhead is further reduced by combining LRE to conglomerate the computation in many system operations.

D. Enhancing Security by CP-ABE

A scheme which ensures data integrity and security in data outsourcing using CP-ABE was suggested [11]. The owner of the data is responsible for defining and enforcing the policies for attributes and not for users. Thus, unauthorized access is 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 are identified by private keys. The key issuing protocol involves key generation and data storing centres. This is 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 involves two authorities, no one can individually generate the secret keys for the user.

E. Hierarchical Attribute-Based Encryption

A new approach namely HABE was invented [3]. By blending HIBE and CP-ABE, HABE can be created for efficient sharing of confidential data on the cloud servers. This is followed by application of PRE and LRE to HABE scheme for the revocation process. This HABE scheme is expected to attain complete delegation, scalability, fine-grained access control and high performance. This system contains the advantages and disadvantages of HIBE and CP-ABE.

F. Attribute Based Encryption in Medical Data Exchange

To make the data exchange secure in cloud, a system was proposed that grants fine grained access control to the outsourced data by combining KP- ABE, PRE and LRE [9]. The purpose of the system is to provide secure access control for medical data exchange and secure key management. This scheme greatly reduces the data owner's difficulties by delegating it to the cloud servers. A medical data exchange scenario has been taken into consideration. Here, the patient wants 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 needs 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 uses his secret key to decrypt the encrypted DEK. Then, the original DEK is used to decrypt the encrypted files. The cloud storage server is assumed to be semi-trusted. This scheme enables data confidentiality, data integrity using authentication, user revocation using lazy encryption and break-glass access in emergency departments.

G. Attribute Based Encryption in Personal Health Records

A centralized storage system with hierarchies was developed for sharing the PHR [13]. PHR is 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 is not good to believe a CA for handling the storage which guides to key escrow problem. To treat this problem, users in the system are classified as personal and public domains. Personal domain deals with the personal information of the patient which is accessible by the data owner. Public domain comprises different types of information. An authority is assigned to each type of information. PHR uses ABE.

Thus, personal domain is controlled by the Data Owner which uses KP-ABE and the public domain is controlled by multiple attribute authorities which use Multiple Authority - Attribute Based Encryption (MA-ABE). The attribute authority is responsible for granting and revoking access to the users. The attributes present in the cipher-text are modified to update the access policies. In Break-glass situations, an emergency department is enclosed which grants temporary read keys to the authorized users in the emergency sites. Scalability and Efficiency are improved in this system which allows secure and scalable sharing of PHRs.

H. 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 are multiple authorities, no central authority is required to manage the entire cloud storage system and it is ensured that the entire security of the cloud storage system is not dependent on the central authority. Temporal Attribute-based Access Control (TAAC) is 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 ciphertext could be avoided.

The purpose of TAAC is to provide time slots and associate the time slot with attributes. The attribute authority can 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 GlobalSetup, AuthoritySetup, 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 are given to those users who possess the attributes. The Update Keys are then published in the public bulletin boards. Secret keys and Update keys are used to generate decryption key for time slot. The four phases in TAAC are System Initialization, Key Generation by Attribute Authorities, Data Encryption by owners and Data Decryption by users. TAAC enhances the scalability and flexibility in constructing an efficient multi authority cloud storage system.

I. Re-Encryption in Unsecured Clouds

A re-encryption scheme was advised to enhance the data security in untrusted clouds [6]. A cloud environment consists of many cloud servers. The authors need to encrypt the data before storing it 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 are rendered to the empowered users. Four cloud servers namely CS1, CS2, CS3 and CS4 have been considered. The data owner wishes to re-encrypt all the old cipher-text using the new re-encryption keys. For this purpose, re-encryption commands are propagated through the entire network. Network

outage takes a chance to prevent the successful re-encryption in all cloud servers. The revoked users gain the old cipher-text which is decrypted by their old decryption keys if the server is not updated due to network failures.

A feasible solution to this problem is 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). The data of Reliable re-encryption scheme in unreliable clouds (R3 scheme) is associated with access time and access control. The design of the R3 scheme is to permit the cloud servers to re-encrypt the data automatically based on the internal clock. This scheme applies 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 meliorates the access control correctness, data consistency, confidentiality and data efficiency.

J. Independent Cloud Systems

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

K. 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 owner of the organization is considered to be the top level user and the employees who are working under the owner are considered to be the lower level users. There is a root-Private Key Generator (root-PKG) which is a trusted third party and it acts 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 grants access to multiple recipients, the system adopts one-to-many encryption and HIBE algorithm.

The hierarchical identity-based architecture consists of a domain which includes the top level user and the lower level user, where the authentication and the secret key transmissions take place. The domain shares the cloud storage services. It is sufficient to store a single cipher-text copy on the cloud, when the sender wants to encrypt and store a file. The file could be recovered by the owner and the concerned people using private keys. The outside attackers and the curious unauthorized employees inside the domain are unable to recover the cipher-text. Collusion attacks are avoided by this scheme. The steps in ESC scheme include RootSetup, DomSetup, One2ManyEnc, UserDec and RecipientsDec. Security and Performance related issues have been given due importance in this scheme.

L. Cloud Storage System Based on Erasure Code

Constructing a secure distributed cloud storage system is a major dispute when it executes multiple functions. Threshold PRE scheme and the decentralized erasure code was suggested for the distributed cloud storage system [10]. The decentralized cloud storage system consists of two servers namely distributed storage servers and key servers. Maintaining separate servers for different functionalities is to ascertain the data confidentiality because the servers are presumed to be semi-trusted. Storage servers perform encoding and forwarding functions while key servers perform partial decryption. Data forwarding uses PRE schemes.

The encryption schemes carry out encoding on the encrypted messages and the forwarding procedures are executed on the encrypted and encoded messages. The four phases in the distributed storage system are System Setup, Data Storage, Data Forwarding, and Data Retrieval. 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 is followed by encryption of the message by user A using user B's public key. The new cipher-text is stored in the cloud for the purpose of forwarding. The cipher-text is 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 attributes are created by the encryptors who encrypt the data. The problem deals with the identification of the person who generates private keys responsible for creating the access policies. In CP-ABE, the user credentials are accepted as attributes, and the encryptors are responsible for creating the access policies. The enhancement of CP-ABE is Ciphertext Policy-Attribute Set Based Encryption (CP-ASBE). In CP-ASBE, the attributes are managed by the recursive set and the users are granted based on the enforcement of the dynamic constraints. The attributes are grouped into sets and the users who possess attributes from those sets have access only to those particular sets. This increases accuracy in confidentiality. In Fuzzy Identity Based Encryption, the identities are chosen as attributes. 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. Identity Based Encryption system associated with hierarchy is HIBE. The private keys are 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. HABE is formed by uniting HIBE and CP-ABE. The extension of CP-ASBE with a hierarchy of users is Hierarchical Attribute Set Based Encryption (HASBE). By analyzing these algorithms, it is decided that HASBE is the upgraded encryption scheme which shares the secured outsourced data in the cloud service provider.

III. CONCLUSION

This paper discusses the cloud storage system and the encryption techniques elaborately. Combination of centralized and decentralized storage systems exist in organizations. Encryption techniques with hierarchies make the storage system more secure and scalable. Implementation of an encryption system on the cloud storage to achieve minimum storage and computation cost provides the necessary impetus for research.

REFERENCES

[1] V.Goyal, O.Pandey, A.Sahai, B.Waters, “Attribute-based encryption for fine grained access control of encrypted data,” CCS., 89–98, 2006.
[2] J.Bethencourt, A.Sahai, B.Waters, “Ciphertext-policy attribute-based encryption,” IEEE S&P., 321–334, 2007.
[3] Guojun Wang, Qin Liu and Jie Wu, “ Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,” CCS Proceedings of the 17th ACM conference on Computer and communications security., 735-737, 2010.
[4] S.Yu, C.Wang, K.Ren and W.Lou, “ Achieving secure, scalable and fine-grained data access control in cloud computing,” IEEE INFOCOM, 2010.
[5] Qin Liu, Guojun Wang and Jie Wu, “ Efficient Sharing of Secure Cloud Storage Services,” 10th IEEE International Conference on Computer and Information Technology, 2010.
[6] Qin Liu, Chiu C.Tan, Jie Wu, and Guojun Wang, “Reliable Reencryption in unreliable cloud," Proc. Of Globecom, 2011.
[7] K.Yang, Z.Liu, Z.Cao, X.Jia, D.S.Wong and K.Ren, “TAAC: Temporal Attribute-based Access Control for Multi- Authority Cloud Storage Systems,” IACR Cryptology ePrint Archive., 651-651, 2012.
[8] B.M.Harish Naik and P.S.Khanagoudar, “A CRM service for cloud computing based on a separate encryption and decryption system,” World Journal of Science and Technology., 2(4):75-80, 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.
[13] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, “ Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,” IEEE Transactions on parallel and distributed systems, Volume 24, No.1, 2013.