ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

Survey on Data Sharing and Re-Encryption in Cloud

Renjith P , Sabitha S

***Abstract*— Cloud storage helps enterprises and government agencies significantly reduce their financial overhead of data management, since they can now archive their data backups remotely to third-party cloud storage providers rather than maintain data centers of their own. Security concerns become relevant as we outsource the storage of possibly sensitive data to third party cloud storage. Data stored in cloud may be unexpectedly disclosed in the future due to malicious attacks on the cloud or careless management of cloud operators. Secure data transfer is needed to maintain the data security between authorized users. The challenge of achieving secure data sharing is that we have to encrypt the data and at the same time it should be available to those authorized clients. This is made possible through re-encryption. The re-encryption process converts the ciphertext encrypted under the public key to a different cipher text encrypted under the intended receiver's public key. The re-encryption is secure only if it does not produce plain text in any of its intermediate stages. The re-encrypting authority should never get any information about the secret keys or the plain text during the process.**

***Index Terms*— Re-encryption, Cloud Storage, Verifiability, Attribute based encryption.**

I. INTRODUCTION

The sensitive data reside in the cloud is in encrypted form. Since data is not physically possessed by the user, security may be violated. Personal Health Record (PHR) normally resides in the cloud in encrypted forms and only authorized parties can access the record. Since different persons need to access the PHR, sharing of PHR is needed which is done through Re-encryption. Re-encryption process converts the cipher text encrypted under sender's public key to cipher text encrypted under receiver's public key using re-encryption key. Cloud data sharing mechanism should ensure that the authorized parties will get the data without any delay which may be incurred due to the Re-encryption process. However the re-encryption process in a cloud computing environment will make the encrypted data available to the intended receiver. This re-encryption process can be made efficient through several methods. The user should get the required data without any performance loss despite of the existence of replicated copies of data in the cloud as well as network problems. The re-encryption process should ensure the integrity of replicated copies. We hereby discuss some of the methods for re- encryption and compare them. The proxy re-encryption method uses a dedicated server or manager for re-encrypting the data. The cloud based re-encryption is performed as a combined effort of more than one managers or servers.

Re-encryption scheme [1] uses key sharing concept which stores the secret key of each user as shares. Secret sharing [8, 9] is typically employed with a distributed service to split the private key among the set of servers. Another improvement in the secret sharing [10] implements a proactive secret sharing method which protects the secrecy of the information by periodically renewing the shares without changing the secret. Thus any information learned by the adversary becomes obsolete after the shares are renewed. Attribute based re-encryption [3] and time based encryption [5] provide better method for data sharing in cloud.

There is a necessity of accountability of the sensitive data. The highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud is introduced in [2] using an object-centered approach. The JAR programmable capabilities are used to both create a dynamic and traveling object, and to ensure that any access to users' data will trigger authentication and automated logging mechanisms. Distributed auditing mechanisms are also provided.

Atomic proxy functions / re-encryption functions are introduced in [11], that convert cipher text for one key into cipher text for another without revealing secret decryption keys or clear text messages. Re-encryption functions can be categorized according to the degree of trust they imply between the two key holders. Re-encryption function by definition allows B to decrypt on behalf of A if and only if A must (unconditionally) trust B. Symmetric proxy functions also imply that B trusts A. Asymmetric proxy functions do not imply this bilateral trust. Symmetric re-encryption scheme using El-gamal encryption is formulated by M. Blaze et. al. in [11].

We can also categorize the asymmetric proxy schemes that might exist according to the convenience in creating the re-encryption key. In an active asymmetric scheme, B has to co-operate to produce the re-encryption key. In a passive asymmetric scheme, on the other hand, A's secret key and B's public key suffice to construct the re-encryption key. Asymmetric proxy re-encryption [12] allows proxy/ manager to transform encrypted messages to cipher text with different recipient public keys. This allows efficient communication to a large no of recipients that are physically

Manuscript received Feb, 2013.

***Renjith P.**, Department of Computer Science and Engineering, College of Engineering Trivandrum. Trivandrum, India, 9446677222.*

***Sabitha S.**, Associate Professor, Department of Computer Science and Engineering, College of Engineering Trivandrum. Trivandrum, India.*

clustered (i.e.; multiparty communication protocols). This scheme will do re-encryption by a single decryption and single encryption using receiver's public key. This process is continued gradually by all quorum servers.

Mambo and Okamoto [13] suggested that there may be more efficient approaches involving partial decryptions, but offered no additional security benefits for Alice's secret key. Blinding [15] is a method of making the data invisible which is the basis for the blinding of el-gamal re-encryption scheme in [17]. El – gamal encrypted secret [16] at sender A is blinded by a random blinding factor which is decrypted using A's private key and finally both encrypted using B's public key. The data is finally un-blinded at B using the original blinding factor.

II. Cloud Background

A. Cloud Data Storage

Cloud storage is the flexible method of storage in which data can be securely stored as use on pay nature. Data stored in the cloud is made secure by cryptographic methods. Cloud allows anywhere access of stored data. Characteristics of secure cloud data storage are Integrity, Availability and Confidentiality. Advantages of cloud storage over traditional server are

- Flexible data access.
- Secure data storage.
- High availability.
- Enhanced sharing.

Sharing is an area of ongoing researches in cloud computing. Sharing can be done by various methods. One of the popular method is to share keys using Diffie-Hellman key exchange method. This shared key can be used to share the data. In a distributed and dynamic scenario this method becomes inadequate. Re-encryption is another method used in data sharing.

B. Re-encryption

Re-encryption is the process of modifying ciphertext encrypted under sender's key to a different ciphertext under receipient's public key. In this process security is maintained only if plain text is not encountered during the re-encryption operation. Blinding process in the encryption does further enhancing of security. Various re-encryption schemes are discussed below.

III. Re-Encryption Methods

A. Secure Erasure Code Based Cloud Storage System with Secure Data Forwarding.

In [1] a specific method of data storage using erasure code is proposed. Erasure coding is the coding method that incorporates error correcting information in data. Each user is assigned a public-secret key pair (PK_a, SK_a) created by the user itself. User distributes his secret key SK_a to key servers such that each key server holds a key share [8]. Encrypted message M is dispatched as shares into storage servers. A message M is decomposed into k blocks and encrypted to cipher shares C_1, $C_2 \ldots C_k$. and sent to randomly chosen storage servers.

During data storage in Storage Servers, erasure code is used for error correction. Codeword symbol is a block of data along with error correcting bits for the specified block. The data forwarding is achieved by using re encryption key. i.e.; the key formed from Secret key (SK_a) of sender (A) and Public Key (PK_b) of receiver (B). Each storage server uses the re-encryption key to re-encrypt its codeword symbol for later retrieval requests by B. In the data retrieval message is either retrieved back by the sender or forwarded to receiver.

For retrieving the data, user A requests key server to retrieve a message from storage servers. The message is either stored by him or forwarded to him. User A sends a retrieval request to key servers. Upon receiving the retrieval request and executing a proper authentication process with user A, each key server requests randomly chosen storage servers to get codeword symbols and performs partial decryption on the received codeword symbols by using the key shares. Finally, user A combines the partially decrypted codeword symbols to obtain the original message M.

This scheme provides

- Secure key sharing.
- Erasure coding.
- Signature verification.
- Reduced user overhead in decryption.

B. Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments

Two types of Attribute Based Encryption (ABE) are Key Policy ABE and Cipher text Policy ABE. In key-policy ABE schemes (KP-ABE), attribute sets are used to annotate cipher texts and private keys are associated with access structures that specify which cipher texts the user will be entitled to decrypt. Cipher text- policy ABE (CP-ABE) proceeds in the dual way, by assigning attribute sets to private keys and letting cipher text specify an access policy that receivers' attribute sets should comply with. Key Policy Attribute Based Encryption is used for fine grained access control over encrypted data. In system [3] the data is stored in the cloud using attribute based encryption. At first the data file is divided into header and body. Body is the ciphertext and header is the encryption key used to encrypt the data into ciphertext. In Attribute Based Encryption data is encrypted by a set of attributes and user secret key are associated with access structure in ABE. Data Encryption Key, DEK is used for encrypting data into body. The header is encrypted using Key Policy -ABE.

The above scheme prevent the collusion attack by dividing and storing data file into header and body. This is achieved by a trusted authority called privilege manager group. That is, the header is sent to privilege manager group, and the body to the cloud service provider. Through this scheme, data confidentiality is guaranteed by the user group since they have to gain admission by privilege manager group. The encrypted data can be accessed from the Cloud Service Provider (CSP). The user can decrypt the encrypted header only if the attribute of the user matches with the access policy specified during the encryption time (of the header). After decrypting the header authorized users obtain the DEK to decrypt the body.

Re-encryption key management can be implemented in two ways – with the key manager or within the cloud. The method proposed in cloud-based re-encryption model [4] is secure, efficient, and highly scalable in a cloud computing context.

This scheme provides

- Attribute Based Encryption.
- Fine grained access.
- Resistant to collusion attack.
- Data Confidentiality.

C. Reliable Re-encryption in Unreliable Clouds

Since a cloud computing environment is comprised of many cloud servers, commands may not be received and executed by all of the cloud servers due to unreliable network communications. In [5] the problem is solved by proposing a time-based re-encryption scheme, which enables the cloud servers to automatically re-encrypt data based on their internal clocks. The solution is built on top of an attribute based encryption (ABE) scheme. ABE allows data to be encrypted using an access structure comprised of different attributes. A cloud is essentially a large scale distributed system where a data owner's data is replicated over multiple servers for high availability. Each cloud server will independently re-encrypt data without receiving any command from the data owner. The method extends an ABE scheme by incorporating timestamps to perform proxy re-encryption. The above solution does not require perfect clock synchronization among all of the cloud servers to maintain correctness.

[5] is a combination of Time based and ABE. Time based user revocation is possible and it handles dynamic data. Data and keys are not divided and shared.

This scheme provides

- Time based re-encryption.
- Attribute Based Encryption.
- User revocation.
- Data confidentiality and efficiency.

Integrity of data which stored in an untrusted server can be verified without retrieving it back in [6]. Utilizing the homomorphic token with distributed verification of erasure-coded data proposed by C.Wang et.al.[7] achieves the integration of storage correctness and data error localization.

D. Quorum controlled asymmetric proxy re-encryption

In Quorum controlled asymmetric proxy re-encryption scheme [12], re-encryption is secure as long as there is no dishonest quorum of proxy servers. This paper introduces the asymmetric proxy re-encryption scheme is an improvement over the previous work [11] Blaze et. al. which is a symmetric proxy encryption. This is an efficient method for multiparty communication since it transforms encrypted message to recipients with different public keys. The recipients can be physically clustered in the network. This method also incorporates publicly verifiable translation certificate which does not reveal any plain text to the reviewer. The re-encryption scheme mentioned here is state as gradual and simultaneous. Each proxy server performs a unit of operation which is the combination of one partial decryption (using a share of the secret key) and one partial encryption (using the intended recipient public key). This process is continued by all proxy servers gradually. In any of the stages of operation, the plain text is not obtained and the system is assumed to be safe. Publicly verifiable translation certificate can be used by the public to verify the correctness of the original message and re-encrypted message. Using translation certificate anyone can verify the correctness of the method without the knowledge of the private key of recipient.

This scheme provides

- Asymmetric re-encryption
- Private key is shared as quorum.
- Verifiable translation certificate.

E. Improved Proxy Re-encryption Scheme.

Improved proxy re-encryption scheme [14] Ateniese et. al. enhances the previous attempts of Blaze et. al. [11]. This method is based on bilinear maps. The encryption process can be customized. With the same public key, the sender is given choice of the recipient set. Re-encryption keys can be generated by sender using receiver's public key; no trusted third party or interaction is required. The algorithm is collusion-resistant, ie., it is hard for the proxy to extract b from re- encryption key, even with the help of Alice (sender).

Features of this scheme are

- Asymmetric re-encryption
- Non interactive
- Collusion resistant
- Unidirectional
- No secret key pre-sharing needed.

F. Distributed Blinding for Distributed ElGamal Re-encryption

Scheme [17] works as a set of distributed services interacting each other for transfer of data from sender to receiver. Blinding [15] is used in the El gamal encryption [16] for masking the data. The decryption process will not reveal the data since it is masked by the blinding factor. Verifiable dual encryption is used to verify the correctness of the re-encrypted data. Asynchronous model of computation is used; there is no bound on message delivery delay.

Features of this scheme includes

- Asymmetric El- gamal re-encryption.
- Distributed asynchronous service.
- Verifiable dual encryption.

IV. COMPARISON

[1] is a simple method of data sharing that does not use either ABE or time based encryption. It directly stores data and keys in servers as shares. Since manager is not present for any transactions between cloud and clients, there is no single point

of vulnerability. No access control mechanisms are implemented to handle revoked users. Owner signature is embedded in the data. The accountability of data can be achieved by the method specified by S. Sundareswaran et. al. [2]. Method proposed in [3] splits data into message body and header and the manager is a single point of vulnerability. [5] is based on automatic time based encryption which doesn't need the trusted manager for re-encryption. [14] is a good solution to the open question introduced in [11] which is the implementation of an asymmetric method for re-encryption. [14] also put forward a new question of unidirectional re-encryption schemes that allow ciphertexts to be re-encrypted in sequence and multiple times. Blinding is introduced in [17] which is El-gamal based re-encryption. Data verifiability is done in [12] using public verifiable translation certificate whereas [17] do the same using verifiable dual encryption. Secure data sharing using re-encryption is well analysed and comparative study is done. Table shows the results.

TABLE I
COMPARATIVE STUDY OF VARIOUS DATA SHARING SCHEMES

	[1]	[3]	[5]	[12]	[14]	[17]
Existence of Manager/Proxy	No	Yes	No	Yes	Yes	Yes
Asymmetric or not	Yes	Yes	Yes	Yes	Yes	Yes
Bilinear mapping	No	Yes	Yes	No	Yes	Yes
Key Shares	Yes	Yes	No	Yes	No	Yes
Blinding	No	No	No	No	No	Yes
Data Verifiability	No	No	No	Yes	No	Yes
Single point of Vulnerability	No	Yes	No	No	No	No

V. CONCLUSIONS

Various data sharing schemes have been analysed and compared. Some methods provide better protection against replay attacks [5] without perfect clock synchronisation. But it has a disadvantage of handling large number of keys. [1] provide better sharing of data using less number of per user keys and resist attacks by key sharing methods. Fine grained access control is provided in [3], [5]. Asymmetric proxy re-encryption methods [12], [14] and [17] are also compared.

ACKNOWLEDGMENT

I would like to express my deep gratitude to my Almighty God, Parents, Guide and all my friends.

REFERENCES

[1] H. Y. Lin and W. Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, pp. 995 – 1003, June 2012.

[2] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring distributed accountability for data sharing in the cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 09, pp. 556–568, July-August 2012.

[3] J.-M. Do, Y.-J. Song, and N. Park, "Attribute based proxy re-encryption for data confidentiality in cloud computing environments," *IEEE International Conference on Computers, Networks*, Systems, and Industrial Engineering, pp. 248–251, 2011.

[4] P. K. Tysowski and M. A. Hasan, "Re-encryption-based key management towards secure and scalable mobile applications in clouds," *IACR Cryptology ePrint Archive*, pp. 668–668, 2011.

[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," *IEEE Globecom 2011 proceedings*, 2011.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 598–609, 2007.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," *Proc. 17th Int'l Workshop Quality of Service (IWQoS '09),* pp. 1–9, July 2009.

[8] G. R. Blakley. Safeguarding cryptographic keys. In Proceedings of the National Computer Conference, 48, pages 313–317. American Federation of Information Processing Societies Pro- ceedings, 1979.

[9] A. Shamir. How to share a secret. Communications of the ACM, 22(11):612–613, November 1979.

[10] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. August 1995. Springer-Verlag.

[11] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," *Advances in Cryptology–EUROCRYPT*, 1998.

[12] M. Jakobsson. On quorum controlled asymmetric proxy re-encryption. In *Proceedings of Public Key Cryptography*. pp. 112-121.

[13] M. Mambo and E. Okamoto. *Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts*. In TFECCS, 1997.

[14] Giuseppe Ateniese, Kevin Fu, Matthew Green and S. Hohenberger Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage, *ACM Transactions on Information and System Security*, Vol. 9, No. 1, February 2006.

[15] D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of Crypto'82*, pages 199–203, 1983.

[16] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[17] Lidong Zhou ; Schneider, F.B. ; Marsh, M.A.; Redz A. Distributed Blinding for Distributed ElGamal Re-encryption, *25th IEEE International Conference on Distributed Computing Systems*, 2005.