Proxy Re-encryption Schemes for Data Storage Security in Cloud- A Survey

W. Sharon Inbarani[1] ,
*PG Scholar,
Department of CSE,
A.S.L Pauls College of
Engineering and
Technology,
India*

G. Shenbagamoorthy[2],
*Assistant Professor,
Department of ECE,
A.S.L Pauls College of
Engineering and
Technology,
India*

C. Kumar Charlie Paul[3],
*Principal,
A.S.L Pauls College of
Engineering and
Technology,
India*

Abstract

A Cloud storage system, consisting of a collection of storage servers, providing long term storage services over the internet. Storing data in a third party's cloud system causes serious concern over data confidentiality. To keep sensitive user data confidential against untrusted servers, cryptographic methods are used to provide security and access control in clouds. As the data is shared over the network, it is needed to be encrypted. There are many encryption schemes that provide security and access control over the network. This paper explores various data encryption techniques such as proxy re-encryption, Type based proxy re-encryption, Key private proxy re-encryption, Identity based proxy re-encryption, Attribute based proxy re-encryption and Threshold proxy re-encryption.

1. Introduction

Cloud computing is emerging as a viable option for internet based development and services. Cloud computing is a distributed computing paradigm where the computing resources such as hardware, software, processing power are delivered as a service over a network. The cloud computing model allows the users to access information and computer resources from anywhere that a network connection is available. The difference between the conventional high performance computing such as grid computing and cloud is that cloud computing has evolved out of grid computing [11] and relies on grid computing as its give backbone and infrastructure support.

Grid computing tends to be loosely coupled, heterogeneous and geographically distributed. The national institute of standards and technology defines cloud computing as follows "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg : networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service providers interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [23]".

In cloud computing all business information and data are stored on distributed servers at remote location. The remote locations are data centres. The client can purchase or rent, such as processing time, network bandwidth, disk storage and memory. Data owners can remotely store their data in the cloud and no longer posses the data locally. Cloud computing moves the application software and database to the large data centre, where the data management and services may not fully trustworthy [3].

A cloud storage system is a distributed storage system [19] which consists of many independent storage servers. The purpose of distributed storage systems is to store data reliably over long periods of time [1]. The main aspect of cloud computing is that many enterprise application are moving into cloud services. The data stored in the cloud is accessed a large number of times and is often subject to different types of changes. An important aspect of cloud storage servers is that, it gives rise to a number of security threats.

Cloud services and applications may require all standard security functions including data confidentiality, integrity, privacy, robustness and access control. Hence providing security to the cloud is the challenging task. There are several cryptographic methods to secure the data stored in cloud storage systems. In this paper encryption technique such as proxy re-encryption (PRE) scheme, Type based PRE, Key-private PRE, Identity based PRE, Attribute based PRE and Threshold PRE are discussed in the following section. The paper has been organized as follows. In section 2 cloud storage infrastructure is discussed. In section 3, PRE scheme is discussed. In section 4, Type based PRE scheme is explained. In section 5, Key-private PRE is analyzed. In section 6, Identity based PRE is discussed. In section 7, Attribute based PRE is explained. In section 8, Threshold PRE is discussed. Finally, in section 9, the conclusion and future work is presented.

2. Cloud Storage Architecture

Typical cloud storage architecture is illustrated in figure 1.

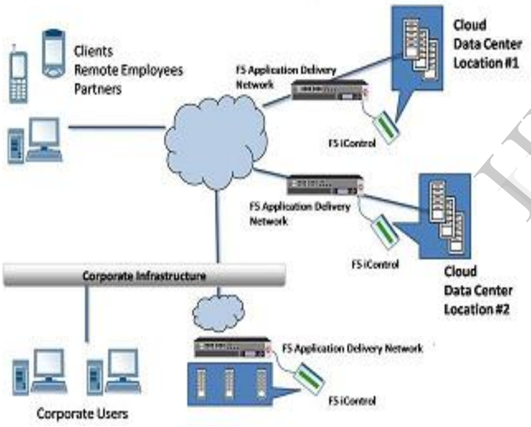

Fig.1.Cloud Storage Architecture

A cloud storage system can be considered to be a network of distributed data centres. The data centres uses cloud computing technologies like virtualization and offers some interfaces for storing useful information. In cloud storage system the owner stores his data, files and application through a CSP (Cloud Service Provider). During file storage, security is one of the main concerns because the data stored on cloud include sensitive information. There can be internal attacks and external attacks. The internal attacks will be within the cloud storage provider itself, whereas the external attack is due to security vulnerabilities which cause data thefts.

The main concept of cloud storage system is to protect the data itself in such a way that even in the event of a successful attack. The content of the data stored in the cloud storage system remain confidential. To provide confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method to encode and store messages [10].

3. Proxy Re-encryption Scheme

The proxy re-encryption schemes are proposed by Mambo and Okamoto [18] and Blaze et al. [16]. Proxy re-encryption is a cryptographic primitive which translates ciphertexts from one encryption key to another encryption key. It can be used to forward encrypted messages without having to expose the cleartexts to the potential users. The re-encryption protocol should be key independent to avoid compromising the private keys of the sender and the recipient. The primary advantage of this PRE [5] scheme is that they are unidirectional (i.e., Alice can delegate to Bob without Bob having to delegate to her) and do not require delegators to reveal their entire secret key to anyone.

A proxy re-encryption algorithm transforms a cipher text under a public key PK_A to cipher text PK_B by using the re-encryption key $RK_{A \rightarrow B.}$ The server does not know the corresponding clear text, where PK_A and PK_B can only be decrypted by different key K_A and K_B respectively. Proxy re-encryption has many applications in addition to the previous proposals [14][24][13][6] for email forwarding, secure network file storage, and performing cryptographic operations on storage limited devices

4. Type Based Proxy Re-encryption Scheme

Type based proxy re-encryption scheme are proposed by Tang [21]. This encryption scheme guarantees data confidentiality and fine gain access control. Type based proxy re-encryption enables the delegator to implement fine grained policies with one key pair without any additional trust on the proxy.

In this scheme the delegator categorizes his ciphertexts into different subsets. Then the decryption right of each subset is delegated to a specific delegate. The ciphertexts for the delegator are generated based on the delegator's public key and the message type which is used to identify the message subset. The type based PRE has the following properties.

1. The delegator only needs one key pair so that key management problem can be simplified.
2. The delegator can choose a particular proxy for a specific delegate, which might be based on the sensitiveness of the delegation. Compromise of one proxy key will only affect one subset of messages.

5. Key Private Proxy Re-encryption Scheme

Key private proxy re-encryption scheme are proposed by Ateniese et al. [5]. In a key private PRE it is impossible for the proxy and a set of colluding users to derive the recipient of a message from the ciphertext and the set of public keys. Achieving key private PRE is only possible when the underlying encryption scheme is key-private. The key privacy encryption provides privacy of the key under which the encryption was performed [17].

The KP-PRE scheme formulates the notion of key-privacy for proxy re-encryption schemes, where even the proxy which performs the translations cannot able to distinguish the identities of the participating parties. In addition to hide the contents of files from the proxy, it is also useful to suppress as much meta-data as possible. For example, we might want the proxy file server to re-encrypt sensitive files for certain recipients without the proxy the recipient's identity.

6. Identity Based Proxy Re-encryption Scheme

The identity based PRE scheme was introduced by Shamir [22]. In an identity based PRE scheme, arbitrary strings such as email addresses or IP address can be used to form public keys for users. In identity based encryption, the senders encrypt messages using the recipient's identity (a string) as the public key. For instance, Alice could encrypt a message for Bob by just using his email address [15].

The identity based proxy re-encryption schemes allow a proxy to translate an encryption under Bob's identity into one computed under Alice's identity. The proxy uses proxy keys, or re-encryption keys, to perform the translation without being able to learn the plaintext. The identity based proxy re-encryption [4] ensures that no reasonable set of colluding key holders will obtain an advantage against non-colluding users. The IBE has a number of practical applications such as secure email forwarding, attribute-based delegations and access control in networked file storage. This type of re-encryption schemes is used to realize the secrecy of data.

6. Attribute Based Proxy Re-encryption Scheme

The concept of attribute based PRE was introduced by Sahai and Waters [2]. In attribute based proxy re-encryption scheme, a semi trusted proxy with some additional information can transform a ciphertext under a set of attributes into a new ciphertext under a set of attributes into a new ciphertext under another set of attributes on the same message. This encryption scheme, allows fine-grained access control on encrypted data. Attribute based encryption is a generalization of IBE. The data provider can express how he wants to share data in the encryption algorithm itself. Goyal et al. [9] introduced two variants of attribute based encryption (ABE) namely ciphertext policy attribute based encryption (CP-ABE) and key policy attribute based encryption (KP-ABE).

In a CP-ABE scheme, a user's private key is associated with a set of attributes and an encrypted ciphertext will specify an access policy over attributes. In KP-ABE [9] scheme, each ciphertext is labelled by the encryptor with a set of descriptive attributes. Each private key is associated with an access structure that specifies which type of ciphertexts the key can decrypt. An important aspect of KP-PRE scheme deals with secure forensic analysis.

In ABE technique, the data is stored on the storage server in an encrypted form while different users are still allowed to decrypt different pieces of data as per security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access.

7. Conditional Proxy Re-encryption Scheme

The Conditional proxy re-encryption (C-PRE) was introduced by Jean Weng and others [12]. The C-PRE scheme involves three principles: a delegator (U_i), a proxy and a delegate (U_j). A message sent to delegator U_i with condition w is encrypted by the sender using both U_i's public key and w. To re-encrypt the message to U_j the proxy is given the re-encryption key ($rk_i \rightarrow j$) and the condition key (ck_i, w) corresponding to w. Both the keys can be generated only by $u_{i.}$ These two keys form the secret trapdoor used by the proxy to perform ciphertext translation. The proxy is unable to translate those ciphertext whose corresponding condition keys are not available. Therefore, U_i has a flexible control on delegation by releasing condition keys properly.

This PRE scheme works in practice as follows: the message encrypted for U_i is first handled by proxy transforms the ciphertext into a ciphertext for $U_{j.}$ However, proxy will obtain no information about the original message. The security requirements for C-PRE systems should ensure that, (i) even if the proxy, who does not have both the partial re-encryption key and the condition key, colludes with the delegate, it is still impossible for them to compromise the delegator's security. (ii) The proxy, who has both the partial re-encryption key and the condition key, compromises neither the delegator not the delegatee's security.

8. Time Based Proxy Re-encryption Scheme

A fundamental approach of Time PRE scheme enables each user's access right to expire automatically after a predetermined period of time [20]. In this case, the data owner can be offline in the process of user revocations. The main idea is to incorporate the concept of time into the combination of Attribute based encryption (ABE) and Proxy re-encryption (PRE).

In time PRE scheme, each data is associated with an attribute based access structure and an access time. Each user is identified by a set of attributes and a set of eligible time periods which denote the period of validity of user's access right. Then, the data owner and the CSP are required to share a root secret key in advance, with which CSP can automatically update the access time of the data with the time that it receives a data access request.

Therefore, given the re-encrypted ciphertext, only the users whose attributes satisfy the access structure and whose access rights are effective in the access time can recover corresponding data. The time PRE scheme enables the CSP to automatically re-encrypt data without receiving any PRE keys from the data owner. This scheme can avoid potential security risks that are raised by the delay of issuing the PRE keys.

8. Threshold Proxy Re-encryption Scheme

A fundamental approach of threshold PRE scheme [8] is for secure computation. This scheme performs arbitrary computations on encrypted data without decrypting it. Threshold PRE technique has multiplicative homomorphic property.A multiplicative homomorphic encryption scheme supports the encoding operation over encrypted messages and forwarding operations over encrypted and encoded messages.

The three properties exhibited by Threshold PRE scheme are : Homomorphism : Given two ciphertexts c1 and c2 on plaintexts p1 and p2 respectively, one can obtain the ciphertext on the plaintext p1+p2 and/or p1.p2 by evaluating c1 and c2 without decrypting ciphertexts.

Proxy re-encryption: Transforming encrypted data of one user to encrypted data of target user.

Threshold decryption: By dividing the private key into several pieces of secret shares, all clients can work together to decrypt the ciphertext – the output of the function.

Based on the above analysis the encryption schemes are tabularized in Table 1 with advantages and disadvantages.

TABLE I
COMPARISON OF DIFFERENT ENCRYPTION SCHEME

No	Encryption Schemes	Advantages	Disadvantages
1	PRE	PRE is secure against plain text attack	Collusion problem and Plaintext attack
2	TB-PRE	Semantic security and ciphertext Privacy Control	Encoding operations over encrypted messages is not possible
3	KP-PRE	Provides CCA security	The key privacy proof is more difficult than that of CPA security
4	IB-PRE	Secure against an adaptive chosen ciphertext attack	Difficult to find efficient constructions for multiuse CCA-secure IBE-PRE.
5	AB-PRE	Fine-grained access control on encrypted data	Average efficiency and flexibility
6	C-PRE	Security against chosen ciphertext attack	It is difficult to design CCA secure C-PRE scheme
7	TB-PRE	1.Scalable user revocation 2.Reduce the workload of the data owner	Requires effective time period to be the same for all attributes associated with the user.
8	T-PRE	Data Forwarding	High access control

9. Conclusion

In cloud computing security is an important aspect of quality of service. To keep the sensitive user data confidential against untrusted servers several proxy re-encryption techniques are used. This paper surveys different proxy re-encryption schemes used in cloud storage system. The advantages and disadvantages of the algorithms have been studied. The future work will be concerned with the development of better PRE schemes which works in distributed environment.

9. References

[1] A. G. Dimakis, P. G. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems" ,IEEE, 2010,pp. 4539-4551.

[2] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption", Springer, 2005, pp. 457–473.

[3] C.Wang, QianWang, KuiRen, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", Proc. IWQoS 09, July 2009, pp. 1–9.

[4] Dan Boneh and Matthew K. Franklin. "Identity-based encryption from the Weil Pairing", In Advances in Cryptology (CRYPTO 2001), Springer, 2001, pp. 213–229.

[5] G. Ateniese, K. Benson, and S. Hohenberger, "Key-Private Proxy Re-Encryption", Proc. Topics in Cryptology, 2009, pp. 279-294.

[6] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger, " Improved Proxy Reencryption Schemes with Applications to Secure Distributed Storage" , In Proceedings of the 12th Annual Network and Distributed System Security Symposium, February 2005.

[7] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage", ACM Trans. Information and System Security, 2006, pp. 1-30.

[8] Gilad Asharov, Abhishek Jain, Adriana Lopez-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs, "Multiparty computation with low communication, computation and interaction via threshold FHE", Proceeding EUROCRYPT'12, Springer, 2012,pp. 483-501.

[9] Goyal V, Pandey O, Sahai A, and Waters B , "Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data", In: ACM conference on Computer and Communications Security, 2006.

[10] Hsiao-Ying Lin and Wen-Guey Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", IEEE, 2012, pp. 995-1003.

[11] Ian Foster,Yong Zhao, Ioan Raicu, and Shiyong Lu, "Cloud Computing and Grid Computing 360-Degree Compared" ,Grid computing workshop, 2008,pp.1-10.

[12] Jian Weng, Robert H. Deng, Xuhua Ding, Cheng-Kang Chu, and Junzuo Lai, " Conditional proxy re-encryption secure against chosen-ciphertext attack", In ASIACCS,2009,pp. 322−332.

[13] Markus Jakobsson, "On quorum controlled asymmetric proxy re-encryption", In Proceedings of Public Key Cryptography, 1999, pp. 112,121.

[14] Matt Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography", In Proceedings of Eurocrypt, 1998, pp. 127–144.

[15] Matthew Green and Giuseppe Ateniese, "Identity-Based Proxy Re-Encryption", ACNS 2007, pp. 288-306.

[16] M. Blaze, G. Bleumer, and M. Strauss,"Divertible Protocols and Atomic Proxy Cryptography", Proc. Int'l Conf. Theory and Application of Cryptographic Techniques ,1998, pp. 127-144.

[17] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval, "Key-privacy in public-key encryption", In ASIACRYPT, 2001, pp. 566-582.

[18] M. Mambo and E. Okamoto, "Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts", IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, 1997, pp. 54-63.

[19] P. Druschel and A. Rowstron, "PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility", Proc. Eighth Workshop Hot Topics in Operating System, 2001, pp. 75-80.

[20] Qin Liu, Guojun Wang and Jie Wu, "Time-Based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment", Information Sciences, In Press, 2012

[21] Q. Tang, "Type-Based Proxy Re-Encryption and Its Construction", Proc. Ninth Int'l Conf. Cryptology in India, 2008, pp. 130-144.

[22] Shamir, "A Identity-based cryptosystems and signatures schemes", In Advances in Cryptology, 1984, pp. 47-53.

[23] The National Institute of Standards and Technology (NIST), Information Technology Laboratory definition of Cloud Computing by Peter Mell and Tim Grance, version 15, October 2009.

[24] Yevgeniy Dodis and Anca Ivan, "Proxy cryptography revisited". In Proceedings of the Tenth Network and Distributed System Security Symposium, February 2003.