International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.06,Issue.13
April-2017,
Pages:2638-2639

www.ijsetr.com

A Survey on Proxy Re-Encryption Scheme for Providing Security in Cloud

R. BHAGYA SRI[1], G. VIJAY KUMAR[2]

[1]PG Scholar, Dept of CSE, G. Pulla Reddy Engineering College (Autonomous), Kurnool, AP, India,
Email: bhagya.rayachuti123@gmail.com.

[2]Assistant Professor, Dept of CSE, G. Pulla Reddy Engineering College (Autonomous), Kurnool, AP, India,
Email: gvjykumar@gmail.com.

Abstract: A Cloud storage system consists a collection of storage servers and provides a long term storage services over the internet. Storing the data in a third party's cloud causes a problem with the data confidentiality. Efficient Conditional Proxy Re-encryption formalizes its semantic security. It allows the sender to encrypt data/message to multiple receivers by providing the receivers' identities. Then the sender sends a re-encryption key to the proxy, so that he/she can convert the cipher text into a new one to the intended receivers' new set. The re-encryption key is associated with a condition such that only the matching cipher texts can be re-encrypted. In a fine-grained manner, it allows the original sender to access control over the cipher texts.

Keywords: Proxy Re-Encryption, Identity-Based Encryption, Conditional Based Proxy Re-Encryption.

I. INTRODUCTION

Encryption is a kind of cryptographic technology which enforces the access control over the encrypted data. It protects the data which is outsourced in the cloud server. The data owner encrypt the data before uploading it to the semi-trusted cloud. One of the most promising approach to protect the data which is stored in cloud is to encrypt these data with asymmetric encryption. To share the data with the other members of the group, the data owner has to download the data and decrypt it. Proxy re-encryption (PRE) enables a semi-trusted proxy to convert a message encrypted under the public key of the sender into another cipher text under the public key of the receiver. However, proxy cannot know the underlying encrypted messages or private keys of sender/receiver. Proxy Re-encryption found in many applications like digital rights management, distributed file storage systems, and email forwarding.

II. RELATED WORK

Initially Blaze [1] introduced the concept of proxy re-encryption called atomic proxy encryption in [1]. In 2003, Ivan and Dodis [2] proposed a unidirectional single-use PRE by splitting the sender's secret key into two different parts and then distributing to the proxy and receiver separately. The original cipher text under the sender's public key cannot be converted into the cipher text intended for the receiver. Shamir [3] introduced an identity based PRE scheme, in this scheme email addresses or IP address 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, sender could encrypt a message for Bob by using their email address .The identity based proxy re-encryption schemes allows a proxy to convert an encryption under receiver's identity into one computed under sender's id. Green et al. [4] introduced the identity based proxy re-encryption (IB-PRE) scheme by incorporating the concept of PRE and ID-based encryption [5]. The PRE scheme proposed is unidirectional, multi-use and non-interactive. But it is not collusion-resistant. Jean Weng [6] introduced the Conditional proxy re-encryption (C-PRE).The C-PRE scheme consists of three principles: a sender, a proxy and a receiver. A message is sent to sender with condition c is encrypted by the sender using both public key and c. The proxy is given the re-encryption key along with the condition key to re-encrypt the message. These keys can be generated by sender and form the secret trapdoor. PRE and IPRE allows only for a single receiver. The system needs to invoke PRE or IPRE multiple times if there are multiple receivers. To solve this problem, the concept of Broadcast PRE (BPRE) has been proposed. BPRE works in a similar way as PRE and IPRE. In contrast, BPRE allows a sender to generate an initial cipher text to a receiver set, instead of a single receiver. This paper proposes a Proxy Re-encryption scheme for secure data sharing and they are organized as follows. **Section I** gives an Introduction. **Section II** gives the related work .**Section III** provides the Architecture. Finally **Section IV** Conclude the paper.

III. ARCHITECTURE

In this scheme, to share the files securely to different receivers, a sender has to encrypt the files with the identities of receiver .The sender sends a re-encryption key with the condition to the proxy. Then the proxy re-encrypts the initial ciphertext matching the condition to the resulting receiver set.

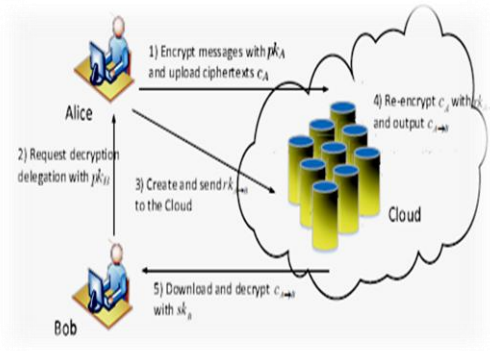

Fig1. Secure data sharing with PRE in cloud computing.

Suppose Alice, the data owner wants to share her secret data stored in the cloud with another user, Bob. The requested data can be accessed only by the intended receiver, Bob. Before uploading the shared data to the semi trusted cloud Alice can encrypt the data under her own public key. Alice generates a proxy re-encryption key using her own private key, after receiving the data request from Bob and sends this proxy re-encryption key to the semi-trusted cloud server. Cloud server transforms the ciphertext encrypted under the public key of Alice into encrypted form under the public key of Bob. This Re-encrypted message can only be decrypted by Bob. Finally, Bob can download the message and decrypt the requested data with his own private key.

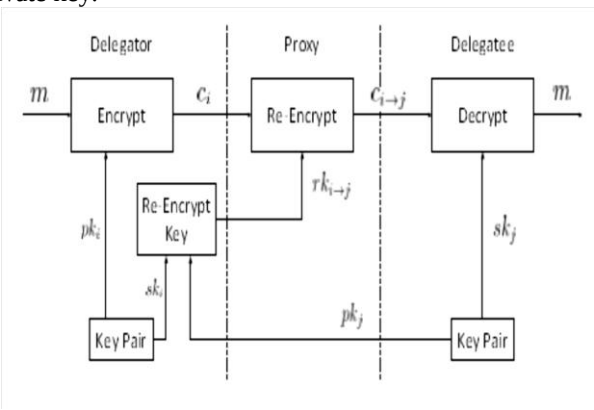

Fig 2. The Intuition of Proxy Re-Encryption Primitive.

Proxy Re-Encryption enables the proxy using a re-encryption key $rk_i \rightarrow j$ to transform a cipher text ci for user i under the public key pk_i into another cipher text cj for user j under the public key pkj on the same message m ∈ M. Then user j is able to obtain the plaintext message m with his/her private key sk_j.

IV. CONCLUSION

A Research is made on efficient proxy re-encryption scheme for secure data sharing. It allows a user to share the encrypted data with other users. All users take their identities as public keys to encrypt data. It avoids a user to fetch and verify other users' certificates before encrypting his data. Moreover, it allows a user to generate a broadcast ciphertext for multiple receivers and share his outsourced encrypted data to multiple receivers in a batch manner.

V. REFERENCES

[1] M. Blaze, G. Bleumer and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography", Proc. Advances in Cryptology- Eurocrypt ' 98, Springer, Heidelberg, 1998, pp. 127-144.

[2] A.-A. Ivan and Y. Dodis, "Proxy cryptography revisited, "in Proceedings of the 2003Symposium on Network and Distributed System Security, 2003

[3] Shamir, A. Palacio and B. Warinschi, "A Closer Look at PKI: Security and Efficiency", Proc. PKC 2007 Springer, Heidelberg, 2007, pp. 458-475.M. Green and G. Ateniese, "Identity-Based Proxy Re-Encryption", Proc. ACNS 2007, Springer, Heidelberg, 2007, pp. 288-306.

[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proceedings of the 2005. Symposium on Network and Distributed System Security,2005.

[5] J. Weng, Y. Yang, Q. Tang, R.H. Deng and F. Bao, "Efficient Conditional Proxy Re-Encryption with Chosen-Ciphertext Security", Proc. Information Security 2009, Springer-Verlag, 2009, pp. 151-166.

[6] J. Shao, G. Wei, Y. Ling and M. Xie, "Identity-based ConditionalProxy Re-encryption", Proc. IEEE International Conference on Communications (ICC), 2011, pp. 1-5.

[7] K. Liang, Z. Liu, X. Tan, D.S. Wong and C. Tang, "A CCA-Secure identity-based conditional proxy re-encryption without random oracles", Proc. ICISC, 2012, pp. 231-146.

[8] C.-K. Chu, J. Weng, S.S.M. Chow, J. Zhou and R.H. Deng, "Conditional Proxy Broadcast Re-Encryption", Proc. Information Security And Privacy 2009, Springer, Heidelberg, 2009, pp. 327-342.

[9] Q. Tang, "Type-Based Proxy Re-encryption and Its Construction", proc. INDOCRYPT, 2008, pp. 130-144.