ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 2 , February 2017

Proxy Re-Encryption for Enhancing Security of Shared Data in Cloud

Dharani R, Theivanai K, Uvalakshmi G

Associate Professor, Information Technology, Panimalar Institute of Technology Poonamallee, Chennai-600123, India
Information Technology, Panimalar Institute of Technology Poonamallee, Chennai-600123, India
Information Technology, Panimalar Institute of Technology Poonamallee, Chennai-600123, India

ABSTRACT*:* In normal Public Key Encryption the data owner needs to download and decrypt the requested data, and further re-encrypt it under the target user's public key which introduces extra computation cost and communication overhead to the data owner and that contradicts the motivation of cloud computing. Another way to think of is to allow data owners to define access policies and encrypt the sharing data with the attribute-based encryption under the access policies, only authenticated users whose attributes matching their policies can decrypt the cipher text. However, here also data owner needs to download, decrypt and re-encrypt the requested data in case data access policies change dynamically and frequently. To overcome these drawbacks Proxy Re-Encryption scheme gives a concrete solution for secure data sharing in cloud computing which deprives user's direct control over the outsourced data. By making cloud server responsible for re-encryption this application reduces communication overhead, extra computational cost which have been introduced to data owners.

KEYWORDS: Proxy Re-Encryption, shared Data, cloud Security, Data Sharing.

I. INTRODUCTION

The rapid development and wide adoption of cloud computing have brought convenience for data storage and sharin. As a representative example, an organization enables its employees in the same group to outsource and share files in the cloud. Fueled by the cloud computing, the employees of the same group can access the shared data that is uploaded by their colleague of the group without any huge capital investments in local storage deployment and maintenance. Furthermore, the shared data which is stored in the cloud can be accessed by any member of the group at any time from any place via Internet. In spite of immense benefits, data sharing in cloud computing is dispossess of user's direct control over the outsourced data, which inevitably enhances security concerns and challenges. Specifically, the outsourced data containing sensitive information should only be accessed by the authorized users. Encryption is a special kind of cryptographic technology that enforces access control over outsourced data [21].

One propitious approach to protect the security of the data stored in cloud computing is to encrypt these data with normal asymmetric encryption owning to the elimination of inconvenient key management in the symmetric encryption. To share storage with many other members of the group, the data owner needs to download and decrypt the requested data, and further re-encrypt it under the data user's public key. In this way, normal public key encryption cannot be regarded as the best candidate to achieve the goal of confidentiality since extra computation cost and communication aerial have been introduced to the data owner, which deny the motivation of cloud computing. Another way to think of is to allow data owners to define access policies and encrypt the sharing data with the attribute-based encryption under the access policies where only authenticated users whose attributes matches these policies can decrypt the ciphertext [13]. However, the data owner also needs to download, decrypt and re-encrypt the requested data in case data access policies change dynamically and frequently.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 2 , February 2017

A. NEED

Data sharing in cloud computing is depriving user's direct control over the outsourced data, which inevitably raises security concerns and challenges. Extra computation cost and communication overhead have been introduced to the data owner. Data owner also needs to download, decrypt and re-encrypt the requested data in case data access policies change dynamically and frequently. To overcome this we use the technique of Proxy Re-Encryption.

II. LITERATURE SURVEY

As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging. [17]present efforts towards storage outsourcing security in cloud computing and describe both our technical approaches and security & performance evaluations. To assure the patients' control over access to their own personal health record PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme. [5]introduce atomic proxy cryptography, in which an atomic proxy function, in conjunction with a public proxy key, converts cipher texts (messages or signatures) for one key into cipher texts for another. Proxy keys, once generated, may be made public and proxy functions applied in untrusted environments. We present atomic proxy functions for discrete-log-based encryption, identification, and signature schemes. It is not clear whether atomic proxy functions exist in general for all public-key cryptosystems. Finally, we discuss the relationship between divertibility and proxy cryptography. [22]look at the problem of interoperability of digital rights management (DRM) systems in home networks. We introduce an intermediate module called the Domain Interoperability Manager (DIM) to efficiently deal with the problem of content and license translation across different DRM regimes. We also consider the threat model specific to interoperability systems, and introduce threats such as the cross-compliancy and splicing attacks. We formalize the adversary model and define security of an interoperable DRM system with respect to this adversary. We finalize by proposing detailed protocols which achieve our security requirements. In order to achieve these requirements we provide novel applications of recently proposed proxy re-signature and proxy re-encryption algorithms.

III. PROPOSED SYSTEM

Proxy re-encryption serves as a promising solution to secure the data sharing in the cloud computing and it overcomes the drawbacks of normal public key encryption and attribute based encryption. They allow to re-encrypt data from one key to another without getting access and to use identities in cryptographic operations. These techniques are used to protect both the data and the authorization model. Each piece of data is ciphered with its own encryption key linked to the authorization model and rules are cryptographically protected to preserve data against the service provider access or misbehaviour when evaluating the rules. As cloud server is made responsible for re-encryption in proxy re-encryption scheme it reduces communication overhead and extra computational cost which have been introduced to data owners.The system can be split into three modules as registration, uploading files and downloading files. In registration, both data user and data owner will register to have login id to access cloud storage. The data owner will upload a file in encrypted format. Data user downloads the file from cloud and decrypts it to view the file

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 2 , February 2017

A. BLOCK DIAGRAM

This special kind of public key encryption seems to be an optimal candidate to ensure the security of sharing data in cloud computing. Suppose the data owner intends to share the sensitive data stored in the cloud with another granted user. It is desirable that the requested data can be accessed by nobody other than Data User. Inspired by the primitive of PRE, Data Owner can encrypt the sensitive data under her own public key before uploading the shared data to the semi trusted cloud. After receiving the request of data sharing from Data User, Data Owner generates a proxy re-encryption key using her own private key and Data User's public key, and sends this proxy re encryption key to the semi-trusted cloud server. Equipped with this proxy re-encryption key, cloud server can transform the cipher text encrypted under the public key of Data Owner into an encryption under the public key of Data User. By utilizing the PRE primitive, the transformed cipher text can only be decrypted by Data User whereas the cloud server is unable to learn the plaintext or private keys of Data Owner or Data User. Finally, Data User can download and decrypt the requested data with his own private key. In this way, the costly burden of secure data sharing can be offloaded to the semi-trusted cloud server with abundant resources. An example of secure data sharing based on PRE is illustrated in Fig. 1.

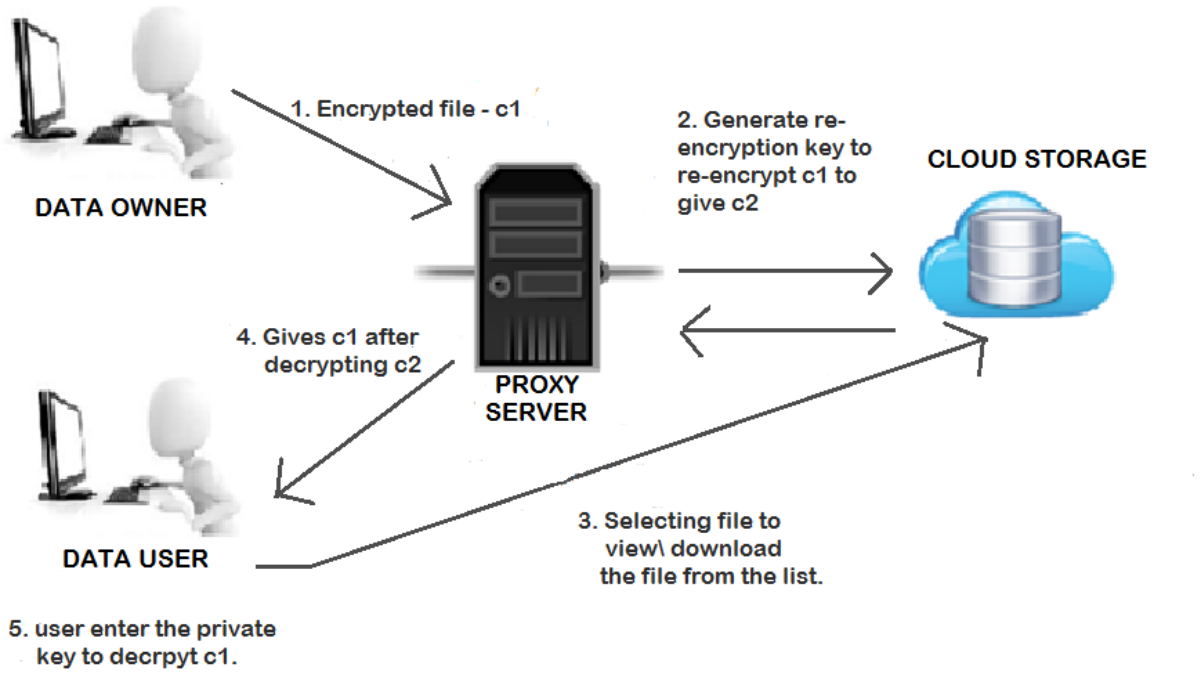

Fig 1. Secure Data Sharing with PRE in cloud computing.

IV. PROXY RE-ENCRYPTION SCHEME

Despite the notion of PRE has been initialized by Blaze *etal.* [5] in 1998, the formal definition and security model for the PRE scheme has been given by Ateniese and Hamburger4] until 2005. By incorporating the definitions by Atenies e*et al*. [2, 3], the syntax for PRE is defined as follows.

Definition 1 (Proxy Re-Encryption): A proxy re-encryption scheme is defined by the following randomized algorithms.• KeyGen: On input the security parameter k ∈K, the key generation algorithm KeyGen outputs a public/private key pair (pk, sk).ReKey: On input a key pair (pu_i, sk_i) for user i and a key pair (pk_j , sk_j) for user j (sk_j is optional), the re encryption key generation algorithm Re Key is performed by user i to output a re-encryption key $rk_j \rightarrow j$. In this case, user i acts as the delegator and user j acts as the delegatee. • Encrypt: On input a plaintext message m ∈ M and a public key pu_j for user i, the encryption algorithm Encrypt outputs an original ciphertext $c_i \in C1$.• ReEncrypt: On input a

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 2 , February 2017

ciphertext ci ∈ C1 for user i and a re-encryption key $rk_{i\rightarrow j}$ for i→ j, the re-encryption algorithm ReEncrypt is performed by the proxy to return a transformed cipher rtext c_j∈ C2 for user j or the error symbol⊥indicating ci is invalid.• Decrypt: On input a private key ski and a ciphertext c_i∈ Cl(l ∈ {1, 2}) for user i, the decryption algorithm Decrypt is performed by user i to output the corresponding plaintext message m ∈ M or a error symbol ⊥indicating ci is invalid. Correctness. Typically, the algorithms of KeyGen, Encrypt and Decrypt in PRE scheme are identical to those of normal public key encryption. For any plaintext m ∈ M and two public/private key pairs (pu_i, sk_i), (pk_j , sk_j) ←KeyGen(k), the correctness of a proxy re-encryption scheme requires that the following equation hold with probability one: Decrypt(sk_i, Encrypt(pu_i,m)) = m, Decrypt(sk_j ,ReEncrypt(ReKey(pu_i, sk_i, pk_j , sk_j), Encrypt(pu_i,m))) = m. As shown in Fig. 2, the aforementioned PRE enables the proxy using a re-encryption key $rk_{i\rightarrow j}$ to transform a ciphertext ci for user i under the public key pu_i into another ciphertext cj for user j under the public key pk_j on the same message m ∈ M. Then user j is able to obtain the plaintext message *m* with his/her private key sk_j . During the execution of a secure PRE scheme, an attacker (e.g. the proxy) cannot learn any information such as the underlying encrypted message m ∈M or private keys (e.g. sk_i or sk_j).

V. DESIGN PHILOSOPHY OF PRE

Unidirectional and Single-use PRE*:* In [2], Ateniese*et al.* [2] proposed an unidirectional and single-use PREscheme (Ateniese [2]-2) based on the bilinear pairings: Theglobal parameters are (p, g, e,G1,G2,Z), where G1 and G2are groups of the prime order *p*, *g* is a random generator ofG1, e : G1 × G1 → G2 and Z = e(g, g) ∈G2.

• (pk, sk) ← KeyGen: On input a security parameter k ∈K, generate a public key pk = (Zx1 , gx2) and a privatekey sk = (x1, x2), where x1, x2 ∈R Zp.

• $rk_{i\rightarrow j}$← ReKey: Given sk_i = (xi1, xi2) for useri (the delegator) and pkj = (Zxj1 , gxj2) for user j (thedelegatee), user i calculates the transformation key $rk_{i\rightarrow j}$ = gxi1xj2 ∈G1.

• ci← Encrypt: To encrypt a plaintext m ∈G2 under the public key pk_i = (Zxi1 , gxi2) for user i, selects a randoms∈R Zp and calculates a ciphertext as follows.– First-Level: Compute and output cx,1 =(Zxi1s,mZs), which can only be decrypted by user i. The first-level cipher text ci,1 can only be decrypted by the delegator.– Second-Level: Compute and output ci,2 = (gs,mZxi1s), which can only be decrypted by user i or the delegatees. The second- level cipher text ci,2 can be decrypted by the delegator and his delegatee.

• ci→j← ReEncrypt: A second-level cipher text under the public key of the delegator can be transformed into a first-level cipher text under the public key of the delegate with the transformation key $rk_{i\rightarrow j}$. Given a re-encryption key $rk_{j\rightarrow j}$ = gxi1xj2 for i→ j and a delegator's second-level ciphertextci,2 = (gs,mZxi1s), the proxy computes e(gs, gxi1xj2) = Zxi1xj2s. Then it produces the re-encryption cipher text ci→j = Zxi1xj2s,mZxi1s) =(Zxj2s′,mZs′) where s′ = xi1s.

• m′ ← Decrypt: On input ski and a ciphertext ci for useri on message *m*,– Given a first-level ciphertext ci,1 for user i and her own private key ski, user i returns m′ =mZs/(Zxi1s)(xi1)−1 . – Given a second-level ciphertext ci,2 for user i and her own private key xi1 ∈ski, user i returns m′ =mZxi1s/e(gs, g)xi1 .In this scheme, the re-encryption key $rk_{i\rightarrow j}$ = (gxj2)xi1 =gxi1xj2 is generated non-interactively by the delegator (e.guser i) with his own private key xi1 and the delegatee (e.guser j)'s public key gxj2 . Then the delegator is responsible for delivering the re- encryption key to the proxy via a secure channel. Compared with Blaze *et al.*'s bidirectional and multi use re-encryption key [5], this scheme is unidirectional and single-use since it is computationally infeasible for the proxy to obtain the re-encryption key $rk_{j\rightarrow i}$ from any other Re encryption keys without user j's delegation. Furthermore, the re-encrypted ciphertext ci→j cannot be re-encrypted by ReEncrypt algorithm any more.Ateniese [2]-2 is a PRE scheme based on bilinear pairings. The Encrypt algorithm contains the first-level encryption and the second-level encryption, where the proxy can only transformed second-level cipher text under the delegator's public key into a first-level cipher text under the delegatee's public key. Meanwhile, the construction of a re-encryption key makes Ateniese [2]-2 non-transitive and collusion-resistant due to the fact that xi cannot be recovered from gxi1xj2 under the discrete logarithm assumption.

VI. CONCLUSION

As a promising primitive to secure the data sharing in the cloud computing, PRE has captured a lot of concern due to the delegation function of decryption. In this paper, we reviewed the state-of-the-art of the PRE by investigating the design philosophy, examining the security models, and comparing the efficiency of existing schemes. Furthermore, the potential applications and extensions of PRE is finding the efficient PRE schemes with full security is also an open problem since most of the existing PRE schemes can only achieve selective security.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 2 , February 2017

REFERENCES

[1] G. Ateniese, K. Benson, and S. Hohenberger, "Keyprivate proxy re-encryption," in *Topics in Cryptology–CT-RSA'09*. Springer, 2009, pp. 279–294.
[2] 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.
[3] ——, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security (TISSEC'06)*, vol. 9, no. 1, pp. 1–30, 2006.
[4] G. Ateniese and S. Hohenberger, "Proxy re-signatures: new definitions, algorithms, and applications," in *Proceedings of the 12th ACM Conference on Computer and Communications Security*. ACM, 2005, pp. 310–319.
[5] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances inCryptology–EUROCRYPT'98*. Springer, 1998, pp. 127–144.
[6] Y.-R. Chen, J. Tygar, and W.-G. Tzeng, "Secure group key management using uni-directional proxy reencryption schemes," in *IEEE International Conference on Computer Communications*. IEEE, 2011, pp. 1952–1960.
[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in Cryptology–CRYPTO'85*. Springer, 1985, vol. 196, pp.10–18.
[8] G. Hanaoka, Y. Kawai, N. Kunihiro, T. Matsuda, J.Weng, R. Zhang, and Y. Zhao, "Generic construction of chosen ciphertext secure proxy re-encryption," in *Topics in Cryptology–CT-RSA'12*. Springer, 2012, pp. 349–364.
[9] A.-A. Ivan and Y. Dodis, "Proxy cryptography revisited," in *Proceedings of the 2003 Symposium on Network and Distributed System Security*, 2003.
[10] M. Jakobsson, "On quorum controlled asymmetric proxy re-encryption," in *2nd International Workshop on Practice and Theory in Public Key Cryptography*. Springer,1999, pp. 112–121.
[11] S. Jun, W. Guiyi, L. Yun, and X. Mande, "Unidirectional identity-based proxy re-signature," in *IEEE International Conference on Communications (ICC 2011)*. IEEE, 2011, pp. 1–5.
[12] S. Lee, H. Park, and J. Kim, "A secure and mutualprofitable drm interoperability scheme," in *Proceedings of IEEE Symposium on Computers and Communications*.IEEE, 2010, pp. 75–80.
[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.
[14] B. Libert and D. Vergnaud, "Unidirectional chosenciphertext secure proxy re-encryption," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1786–1802, 2011.
[15] D. Nunez, I. Agudo, and J. Lopez, "A parametric family of attack models for proxy re-encryption," in *IEEE 28th Computer Security Foundations Symposium (CSF 2015)*. IEEE, 2015, pp. 290–301.
[16] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in *33rd International Convention on Information and Communication Technology, Electronics and Microelectronics*. IEEE, 2010, pp. 344–349.
[17] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, no. 1, pp. 69–73, 2012.
[18] J. Shao, P. Liu, Z. Cao, and G. Wei, "Multi-use unidirectional proxy re-encryption," in *IEEE International Conference on Communications*. IEEE, 2011, pp. 1–5.
[19] J. Shao, P. Liu, and Y. Zhou, "Achieving key privacy without losing cca security in proxy re-encryption," *Journal of Systems and Software*, vol. 85, no. 3, pp. 655–665, 2012.
[20] J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in *IEEE InternationalConference on Communications*. IEEE, 2011, pp. 1–5.
[21] 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. 9, no. 4, pp. 556–568, 2012.
[22] G. Taban, A. A. C´ardenas, and V. D. Gligor, "Towards a secure and interoperable drm architecture," in *Proceedings of the ACM Workshop on Digital Rights Management*. ACM, 2006, pp. 69–78.
[23] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, "Efficient conditional proxy re-encryption with chosenciphertext security," in *Proceedings of the 12th International Conference on Information Security*. Springer, 2009, pp. 151–166.
[24] J. Weng, Y. Zhao, and G. Hanaoka, "On the security of a bidirectional proxy re-encryption scheme from pkcb 010," in *Public Key Cryptography–PKC'11*. Springer, 2011, pp. 284–295.
[25] T. Yang, H. Xiong, J. Hu, Y. Wang, W. Xin, Y. Deng, and Z. Chen, "A traceable privacy-preserving authentication protocol for vanets based on proxy re-signature," in *8th International Conference on Fuzzy Systems and Knowledge Discovery*, vol. 4. IEEE, 2011, pp. 2217–2221.