© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Proxy Re-Encryption Technique for Attaining Privacy

Raghapriya S, Sandhiya D, Ms. Subhashini A

Computer Science and Engineering, Dhanalakshmi College of Engineering, Tambaram, Chennai, Tamil Nadu, India

ABSTRACT

Security is a prime concern for any service that provides big data storage. The data of an individual should remain confidential and should be accessed only by any authenticated person. One of the aspects of security that is considered prior storing data is the anonymity of the service clients. The service that is used for storage should provide practical and fine-grained encrypted data sharing in such a way that only a ciphertext of data is shared among others by the data owner under some specified conditions. The required features are obtained by introducing a new technique for providing big data storage i.e. a privacy-preserving ciphertext multi-sharing mechanism. In this technique the advantages of proxy re-encryption technique are employed that enables ciphertext to be securely and conditionally shared multiple times and it also ensures that the knowledge of underlying message and the identity information of ciphertext senders and recipients is not leaked. The technique is also vulnerable to the chosen-ciphertext attacks.

Keywords: Automatic Packet Generation, Fault Node Recovery, Dynamic Testing

I. INTRODUCTION

To date many individuals and companies choose to upload their data to clouds since the clouds supports considerable data storage service but also efficient data processing capability. Accordingly, it is unavoidable that trillions of personal and industrial data are flooding the Internet. For example, in some smart grid scenario, a governmental surveillance authority may choose to supervise the electricity consumption of a local living district. A great amount of electricity consumed data of each family located inside the district will be automatically transferred to the authority via Internet period by period. The need of big data storage, therefore, is more desirable than ever.

A basic security requirement of big data storage is to guarantee the confidentiality of the data. Fortunately, some existing cryptographic encryption mechanisms can be employed to fulfill the requirement. For instance, Public Key Encryption (PKE) allows a data sender to encrypt the data under the public key of receiver such that no one except the valid recipient can gain access to the data. Nevertheless, this does not satisfy all the requirements of users in the scenario of big data storage. We suppose a hospital stores its patients' medical records in a cloud storage system and meanwhile, the records are all encrypted so as to avoid the cloud server from accessing to any patient's medical information. After a record is encrypted and further uploaded to the cloud, only those specified doctors can gain access to the record. By using some traditional PKE, Identity-Based Encryption (IBE), or Attribute-Based Encryption (ABE), the confidentiality of the record can be protected effectively.

By trivially employing traditional encryption mechanisms (to guarantee the confidentiality of medical record), nevertheless, we cannot prevent some sensitive personal information from being leaked to the cloud server but also the public. This is because traditional encryption systems do not consider the anonymity of a ciphertext sender/receiver. Accordingly, someone could be anyone with capability of obtaining a ciphertext (e.g. cloud server), may know whose public key the ciphertext is encrypted under, namely who is the owner of the ciphertext, such that the patient associated with the ciphertext can be easily identified.

Similarly, the recipient/destination of the ciphertext, e.g., Cardiology Dept., can be known from the ciphertext without any difficulty as well. This seriously disgraces the privacy of patient. Moreover, a patient might be transferred to more than one medical department in different treatment phases. The corresponding medical record then needs to be converted to the ciphertexts corresponding to various receivers so as to be shared among the departments.

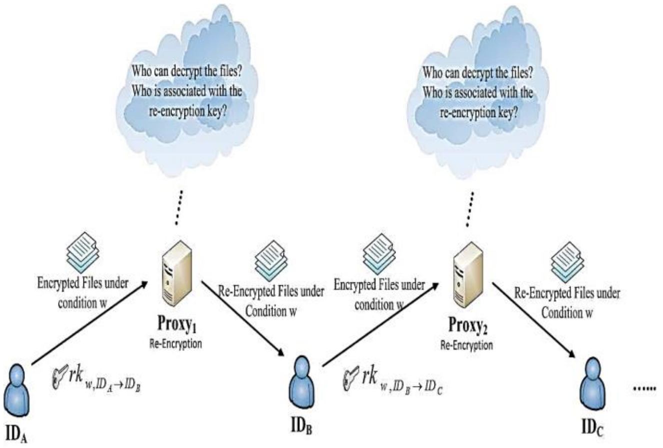
Who can decrypt the files?
Who is associated with the re-encryption key?
Who can decrypt the files?
Who is associated with the re-encryption key?
Encrypted Files under condition w
Proxy$_1$
Re-Encryption
Re-Encrypted Files under Condition w
Encrypted Files under condition w
Proxy$_2$
Re-Encryption
Re-Encrypted Files under Condition w
$rk_{w,ID_A \to ID_B}$
$rk_{w,ID_B \to ID_C}$
ID$_A$
ID$_B$
ID$_C$
......

Figure 1. Anonymous Multi-Hop Identity-Based Conditional Proxy Re-Encryption

Therefore, the update of ciphertext recipient is desirable. Precisely speaking, a fine-grained ciphertext update for receivers is necessary in the sense that a ciphertext can be conditionally shared with others. The medical record owner, e.g., the patient, has rights to decide who can gain access to the record, and which kinds of data are allowed for access. For example, the patient can choose to specify that only the medical record described with "teeth" can be read by a dentist. This fine-grained control prevents a data sharing mechanism from being limited to the "all-or-nothing" share mode.

This research work aims to solve the above problems. To preserve anonymity, some well-known encryption mechanisms are proposed in the literature, such as anonymous IBE. By employing these primitives, the source and the destination of data can be protected privately. However, the primitives cannot support the update of ciphertext receiver. There are some naive approaches to update cipher text's recipient. For instance, data owner can employ the decrypt then re-encrypt mode. Nonetheless, this is applicable to the scenario where there is only a small amount of data. If the encrypted data is either a group of sequences of genome information or a network audit log, the decryption and re-encryption might be time consumed and computation costly. Moreover, this mode also suffers from a limitation that the data owner has to be on-line all the time. Alternatively, a fully trusted third party with knowledge of the decryption key of the data owner may be delegated to handle the task. Nevertheless, this strongly relies on the fully trust of the party.

Besides, the anonymity of the ciphertext receiver cannot be achieved as the party needs to know the information of recipient to precede the re-encryption. Therefore, both of the approaches do not scale well in practice. Introduced by Mambo and Okamoto and further defined in Proxy Re-Encryption (PRE) is proposed to tackle the dilemma of data sharing.

It allows a semi-trusted party, called proxy, to transform a ciphertext intended for a user into a ciphertext of the same message intended for another user without leaking knowledge of either the decryption keys or the message. The workload of data owner is now transferred to the proxy, and the "on-line all the time" requirement is unnecessary. This work concentrates on the identity-based cryptographic setting. To employ PRE in the IBE settings defined the notion of Identity-Based Proxy Re-Encryption (IBPRE), which offers a practical solution for access control in networked file storage and secure email with IBE.

To capture privacy-preserving property and ciphertext's recipient update simultaneously, [30] proposed an anonymous IBPRE system, which is CCA security in the Random Oracle Model (ROM). The valuable work introduces the first anonymous IBPRE in the literature and meanwhile, it leaves us interesting and meaningful open problems. The work only supports one-time ciphertext receiver update, while multiple receivers update is desirable in practice. On the other hand, the work provides an "all-or-nothing" share mode that limits the flexibility of data sharing.

- **Anonymity**: Given a ciphertext, no one knows the identity information of sender and receiver.

- **Multiple receiver-updates**: Given a ciphertext, the receiver of the ciphertext can be updated in multiple times. It refers to this property as “multi-hop”.
- **Conditional sharing**: A ciphertext can be fine-grained shared with others if the pre-specified conditions are satisfied.
- **Achievements**: We investigate a new notion, AMH-IBCPRE. We formalize the definition and security model by incorporating the definitions.

II. METHODS AND MATERIAL

A. Existing System

- An identity-based proxy re-encryption scheme with source hiding property, and its application to a mailing-list system.
- The anonymity of the service clients, one of the most essential aspects of privacy, should be considered simultaneously.
- Fine-grained encrypted data sharing such that a data owner is allowed to share a ciphertext of data among others under some specified conditions.
- Normal encryption and decryption method used.

B. Drawbacks

- In existing system the patient any time monitoring the system.
- Not secure.
- The patient should remember the key.

C. Proposed System

- It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of ciphertext senders/recipients.
- It is secure against chosen-cipher text attacks.
- We use AES (Advanced Encryption Standard) and Random Key Generation method is to be used for encryption, decryption and key generation.

D. Benefits of Proposed System

- More secure compared to existing method.
- Proxy Re encryption method used so it is act as a user.
- No need to monitor the system and key any time.

E. System Architecture

Data Owner is the one who maintains the patient’s record and he provides the encryption key for each patients. The data owner stores the encryption key for the patient in the proxy server. The proxy server will display the information only when the encryption key is valid for that particular patient. The main advantage of this proxy re-encryption technique is that the doctor can get information about the patients at any time at any cause. In this process there is no need to monitor the system and key at any time. Proxy re-encryption plays a vital role in this process which overcomes the drawbacks of existing system.

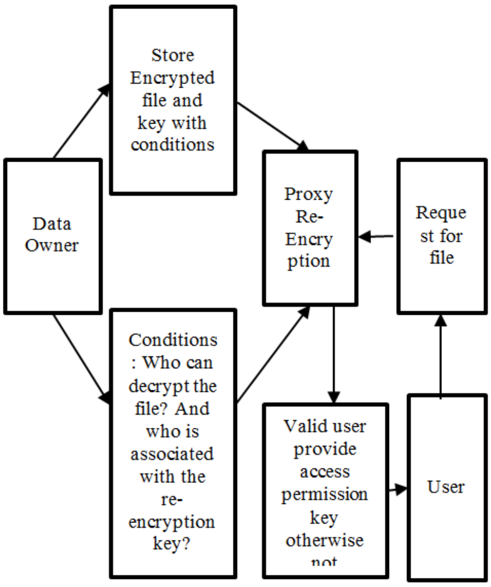
Store Encrypted file and key with conditions
Data Owner
Proxy Re-Encry ption
Reque st for file
Conditions : Who can decrypt the file? And who is associated with the re-encryption key?
Valid user provide access permission key otherwise not
User

Figure 2. System Architecture

III. RESULTS AND DISCUSSION

Module Description

There are three modules following

1. Data Outsourcing
2. Data Sharing
3. Proxy Re-Encryption

A. Data Outsourcing

- The Data Owner stores the data into the cloud.

- That the data is either public or private.
- Data is private means; the data is converted encrypted form using some encryption methods.

B. Data Sharing

- It is used to share the data to the specific consumer.
- In this process, information about the particular patient is stored in a database and encryption key is given for each patient.
- The doctor checks the information about the patient using the proxy server; the proxy re-encryption technique displays the information about that particular patient if the key is validated with the patient records.

C. Proxy Re-Encryption

- Its act as a Data Owner and it is used to check the concern person is valid person or not valid person.
- The person is valid means it provide the access Key otherwise not provide.

IV. CONCLUSION

It introduced a novel notion, anonymous multi-hop identity-based conditional proxy re-encryption, to preserve the anonymity for ciphertext sender/receiver, conditional data sharing and multiple recipient update. We further proposed a concrete system for the notion. Meanwhile, we proved the system CCA-secure in the standard model under the decisional P-bilinear Diffie Hellman assumption. To the best of our knowledge, our primitive is the first of its kind in the literature.

V. REFERENCES

[1] M. Mambo and E. Okamoto, "Conditional Identity-based Broadcast Proxy Re-Encryption and Its Application to Cloud Email" IEICE Trans. Fundam. Electron.,Commun., Comput. Sci., vol. E80-A, no. 1, pp. 54–63, 1997.

[2] X. Boyen and B. Waters, "Anonymous hierarchical identity- based encryption (without random oracles)," in Advances in Cryptology–CRYPTO (Lecture Notes in Computer Science), vol. 4117. Berlin, Germany: Springer-Verlag, Aug. 2006, pp. 290–307.

[3] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," inPublic Key Cryptography, vol. 4939. Berlin, Germany: Springer-Verlag, 2008, pp. 360–379.

[4] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," inAdvances in Cryptology– CRYPTO (Lecture Notes in Computer Science), vol. 5677. Berlin, Germany: Springer-Verlag, 2009, pp. 619–636.

[5] K. Emura, A. Miyaji, and K. Omote, "An identity-based proxy re-encryption scheme with source hiding property, and its application to a mailing-list system," in Public Key Infrastructures, Services and Applications,vol. 6711. Berlin, Germany: Springer-Verlag, 2011, pp. 77–92.

[6] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Oct. 2007, pp. 185–194.

[7] A. Ivan and Y. Dodis, "Proxy cryptography revisited," in Network and Distributed System Security. Berlin, Germany: Springer-Verlag, 2003.

[8] X. Boyen and B. Waters, "Anonymous hierarchical identity- based encryption (without random oracles)," in Advances in Cryptology– CRYPTO (Lecture Notes in Computer Science), vol. 4117. Berlin, Germany: Springer-Verlag, Aug. 2006, pp. 290–307.

[9] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 5443. Berlin, Germany: Springer - Verlag, 2009, pp. 196–214.

[10] R. Canetti, S. Halevi, and J. Katz, "Chosen - ciphertext security from identity-based encryption," in Advances in Cryptology – EUROCRYPT (Lecture Notes in Computer Science), vol. 3027. Berlin, Germany: Springer-Verlag, 2004, pp. 207–222.

[11] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS) Oct. 2007, pp. 185–194.

[12] C.-K. Chu and W.-G. Tzeng, "Identity-based proxy re-encryption without random oracles," in Information Security (Lecture Notes in Computer Science), vol. 4779. Berlin, Germany: Springer-Verlag, 2007, pp. 189–202.

[13] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," SIAM J. Comput., vol. 33, no. 1, pp. 167–226, Jan. 2004.

[14] L. Ducas, "Anonymity from asymmetry: New constructions for anonymous HIBE," in Topics in Cryptology–CT-RSA (Lecture Notes in Computer Science), vol. 5985. Berlin, Germany: Springer-Verlag, 2010, pp. 148–164.

[15] K. Emura, A. Miyaji, and K. Omote, "An identity-based proxy re-encryption scheme with source hiding property, and its application to a mailing-list system," in Public Key Infrastructures, Services and Applications (Lecture Notes in Computer Science), vol. 6711. Berlin, Germany: Springer-Verlag, 2011, pp. 77–92.