IDENTITY BASED CASCADE ENCRYPTION IN CLOUD EMAIL APPLICATIONS

B.Gowsalya, M.Kanmani & V.Kanagalakshmi
Students, Department of Computer Science and Engineering,
P.S.R Rengasamy College of Engineering for Women, Sivakasi, Tamilnadu, India

S.Grahalakshmi
Assistant Professor, Department of Computer Science and Engineering,
P.S.R Rengasamy College of Engineering for Women, Sivakasi, Tamilnadu, India

Abstract

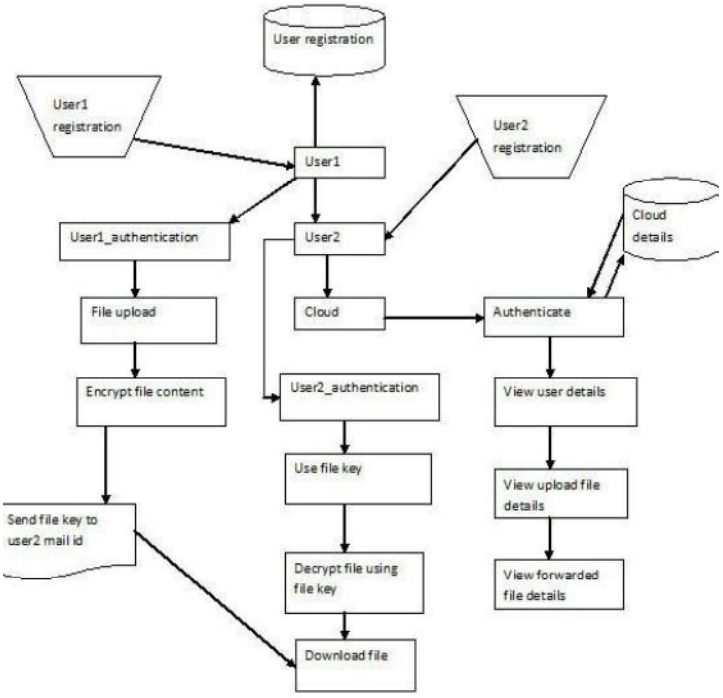
The CIBPRE can allow a sender to encrypt a message to multiple receiver's .Then sender can representative a re-encryption key to a proxy so the initial cipher text can convert into a new set of intended receivers. The re-encryption key can be related to a condition only matching the cipher texts can be re-encrypted. It allows the original sender to implement the access control. The re -encryption key are all in constant size, and then parameters can generate a re-encryption key all are independent of the original receivers. CPRE, IPRE and BPRE, this paper propose a multifaceted primitive referred to as conditional identity-based broadcast PRE (CIBPRE) and formalizes its semantic security. In addition the random key algorithm can be used and it can generate a random key. This key provides a more secure for encrypted message. Then multi sharing algorithm also uses and its work is multiple message can send securely to multiple receivers.

Key word: *Proxy re-encryption, conditional based proxy re-encryption, identity based proxy re-encryption*

Introduction

Proxy re-encryption (PRE) provides a secure and flexible method for a sender to store and share data. A user may encrypt the file with the own public key and then store the cipher text in a server. When the receiver is certain, the sender can assign a re-encryption key related with the receiver to the server as a proxy. Then the proxy re-encrypts the initial cipher text to the intended receiver. Finally, the receiver can decrypt the resultant cipher text with private key. The security of PRE usually assures that neither the server/proxy nor non-intended receiver's can learn any useful information about the re-encrypted file, and before receiving the re-encryption key, the proxy cannot re-encrypt the initial cipher text in a meaningful way. The early PRE was proposed in the traditional public- key infrastructure setting which incur complicated certificate management. To relieve from this problem, several identity- based PRE (IPRE) schemes were proposed so that the receiver's identifiable identities can serve as public keys. Instead of fetching and verifying the receiver's certificates, the sender and the proxy just need to know the receivers identities, which is more convenient. PRE and IPRE allow a single receiver. If there are more receivers, the system needs to raise PRE or IPRE multiple times. To address this issue, the concept of broadcast PRE (BPRE) has been proposed. BPRE works in a similar way as PRE and IPRE but more versatile. In contrast, BPRE allows a sender to generate an initial cipher text to a receiver set, instead of a single receiver. A recent conditional proxy broadcast re-encryption scheme allows the senders to control the time to

re encrypt their initial cipher texts. When a sender generates a re-encryption key to re-encrypt an initial cipher text, the sender needs to take the original receivers identities of the initial cipher text as input. In apply, it means that the sender must close by remember the receiver's identities of all initial cipher texts. This condition makes this scheme controlled for the memory-limited applications. Then describe a convenient security notion for CIBPRE systems. The consequent private keys one can learn nothing about the plaintext secreted in the initial or re-encrypted CIBPRE cipher text, an initial cipher text cannot be correctly re-encrypted by a re -encryption key if the cipher text and the key are related with different conditions. In this project we are going to generate a key and send that key to our mail using the random key algorithm.



System Flow Diagram

Proposed System

Random key algorithm is used in this project for more security purpose in file sharing. It can generate the random key .That can be communicated from one sender to multi receiver. Multi sharing algorithm is also used for sharing multiple files in multiple receivers . It allows a user to share their outsourced encrypted data with others in a fine-grained manner. All CIBPRE 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 cipher text for multiple receivers and share his outsourced encrypted data to multiple receivers in a batch manner.

Existing System

We refine PRE by incorporating the advantages of IPRE, CPRE and BPRE for more flexible applications and propose a new concept of conditional identity based broadcast PRE (CIBPRE).To

securely share files to multiple receivers, a sender can encrypt the files with the receivers' identities and file-sharing conditions. It share single file to multiple receivers. The early PRE was proposed in the traditional public- key infrastructure setting which incurs complicated certificate management.

Related Work

These PRE schemes need certificates to prove the validity of public keys. A user has to verify the certificates before encrypting a plaintext. In order to avoid the overhead to verify public keys. Then verified secure in the random key (Rk) model in which a hash function is understood fully random. The above PRE schemes only allow data sharing in a coarse-grained manner. Than it the user delegates are encryption key to the proxy, all cipher texts can be re encrypted and then be accessible to the intended users, else none of the cipher texts can be re- encrypted.

Modules

To get the information from the users. The information are stored in the server. Key generation is the process of generating keys. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted. When a new user joins this system, the KGC generates a private key. Without loss of generality, let ID denote the email address of the new user. To generate the private key, and sends it to the user in a secure channel which is established by the SSL/TLS protocol. A user can send an encrypted email to other users this email will be stored in the cloud server. If the user wants to review this email, he can fetch the encrypted email from the cloud server and decrypt it.

Re-Encryption

Re-encryption is the process of modifying cipher text encrypted under sender's key to a different cipher text under recipient's public key. In this process security is maintained only if plain text is not encountered through the re-encryption operation. Blinding process in the encryption does additional enhancing of security. A user 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.

Proxy Re-Encryption

The proxy re-encryption scheme enhances the preceding attempts. This method is based on bilinear maps. The encryption process can be personalized. With the same public key, the sender is given option of the receiver set. Re-encryption keys can be generated by sender using receiver's public key; no trusted third party or interaction is necessary.

The algorithm is collusion-resistant it is hard for the proxy to extract b from re- encryption key. Features of this scheme are

Asymmetric re-encryption

Non interactive

Collusion resistant Unidirectional

No secret key pre-sharing needed

Cloud Data Storage

Cloud storage is the flexible method of storage in which data can be securely stored as use on recompense nature. Data stored in the cloud is made secure by cryptographic methods. Cloud allows wherever access of stored data. Description sof secure cloud data storage is Integrity, accessibility and privacy. Advantages of cloud storage over traditional server are

Flexible data access. Secure data storage. High accessibility.

Enhanced sharing.

Conditional based Proxy Re-Encryption

Proxy re-encryption can be used in applications where delegation is required, for an example in case of delegated email processing. But, it is not enough to handle scenarios where a fine-grained delegation is demanded. For example, john is only allowed Lisa's encrypted emails containing a predetermine keyword. In order to overcome the limitation of existing PRE, in [13] the system introduces the notion of conditional proxy re-encryption (or C-PRE), whereby only cipher text satisfying one condition set by Alice can be transformed by the proxy and then decrypted by john. The author formulates its security model

Key Private Proxy Re-Encryption

In many applications, to protect data with one public key pk1 requires to be disseminated to every user with a unique public key pk2. This becomes little impractical for the owner of sk1 to be online to decrypt these cipher texts and then encrypt these contents under a new key pk2.A key-private re-encryption keys as an additional property that enhances the PRE schemes, the authors defines PRE scheme to be secure and key-private. Unexpectedly, the system show that this property is not achieved by previous schemes, also even after including the secure the communication from being harder to interpret PRE. Finally, the author conclude by proposing one of the unique feature of the first key-private PRE construction and prove its CPA-security under a simple extension of Decisional Bilinear Diffie-Hellman assumption and its key-privacy under the Decision Linear assumption in the standard model and also proposes an efficient C- PRE scheme, whose chosen-ciphertext security is proven under the 3-quotient bilinear Diffe- Hellman assumption.

Conclusion

In this paper any file to be encrypted and then again re encrypted and the fisnally key will be stored in cloud. The key is sent by the cloud through sender mail. Then the sender can recognize the receiver. Sender sends the key to the receiver and then key in the cloud will automatically send to the receiver. When the two keys are matched then only the file will be opened.

Acknowledgment

I would like to express my profound gratefulness to my Almighty God, Parents, Guide and all my friends

Reference

1. M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Crytographic Techn.: Adv. Cryptol., 1998, pp. 127–144.
2. A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi, "A closer look at PKI: Security and efficiency," in Proc. 10th Int. Conf. Practice Theory Public-Key Cryptography, 2007, pp. 458–475.
3. M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proc. 5th Int. Conf. Appl. Cryptography Netw. Security, 2007, pp. 288–306.
4. T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 247–267.
5. C.-K. Chu and W.-G. Tzeng, "Identity-based proxy re-encryption without random oracles," in Proc. 10th Int. Conf. Inf. Security, 2007, pp. 189–202.
6. L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "A type-and-identitybased proxy re-encryption scheme and its application in healthcare," in Proc. 5th VLDB Conf. Secure Data Manage., 2008, pp. 185–198.
7. J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in Proc. IEEE Int. Conf. Commun., 2011, pp. 1–5.
8. K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang, "A CCA-secure identity-based conditional proxy re-encryption without random oracles," in Proc. 15th Int. Conf. Inf. Security Cryptol., 2012,pp. 231–146.
9. C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, "Conditional proxy broadcast re-encryption," in Proc. 14th Australasian Conf. Inf. Security Privacy, 2009, pp. 327–342.
10. Q. Tang, "Type-based proxy re-encryption and its construction," in Proc. 9th Int. Conf. Cryptol. India: Progress Cryptol., 2008,pp.130–140