International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Secure Operations of Cloud Email System by Using Contingent ID-Based Transmission Proxy Double-Encryption Technique

Dr. Mohammed Abdul Waheed[1], Vrushabha Lingaraja[2]

[1]Associate Professor, Department of Studies in Computer Science and Engineering, Visvesvaraya Technological University. CGPS, Kalaburagi, Karnataka, India

[2]Mtech Student, Department of Studies in Computer Science and Engineering,Visvesvaraya Technological University, CGPS, Kalaburagi, Karnataka, India

ABSTRACT

Firstly, various expanded Proxy Re-Encryptions (PRE), e.g. Contingent (CPRE), ID-based PRE (IPRE) and communicate PRE (BPRE), have been proposed for adaptable applications. By joining CPRE, IPRE and BPRE, this paper proposes an adaptable primitive alluded to as contingent ID-based communicate double encryption and formalizes its semantic security. New proposed system enables a sender to scramble a message to numerous recipients by indicating these receiver's personalities, and the sender can assign a re-encryption key to an intermediary/proxy with the goal that he can change over the underlying Cipher-Text into another one to another set of planned collectors. In addition, the re-encryption key can be related with a condition to such an extent that only the coordinating Cipher-Texts can be re-scrambled, which enables the first sender to authorize get to control over his remote Cipher-Texts in a fine-grained way. We propose an effective system conspire with provable security. In the instantiated plot, the underlying Cipher-Text, the re-encoded Cipher-Text and the re-encryption enter are all in consistent size, and the parameters to produce a re-encryption key are autonomous of the first recipients of any underlying Cipher-Text. At last, we demonstrate a utilization of our proxy double encryption to secure cloud email framework profitable over existing secure email frameworks in view of Pretty Good Privacy convention or personality based encryption.

Keywords: Proxy Double-Encryption, Cloud Storage, Identity-Based Encryption, Broad Cast Encryption, Secure Cloud Email

I. INTRODUCTION

PROXY double encryption provides a secure and flexible method for a sender to store the data and share the data. A user can encrypt his file by make use of his own public key and then store the resulting cipher-text in an honest-but-curious server. When the intended receiver is decided, the sender can delegate a re-encryption key which is associated with the receiver to the server as a proxy. Then the proxy will change the data by re-encrypting the initial cipher-text to the intended receiver. Finally, the receiver can decrypt the resulting cipher-text with her private key. The security of PRE usually assures that (1) Neither the server/proxy nor non-intended receivers can learn any useful information about the re-encrypted file, nor
(2) 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 incurs complicated certificate management. The traditional PRE schemes only allow data sharing in a coarse-grained manner. That is, if the user delegates a re-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 or accessed by others. PGP and IBE, system is less efficient in the aspect of

communication and not more practical in user experience. Users are not able to share the encrypted data to others, lot of issue are occurring.

II. LITERATURE SURVEY

1) Identity-Based Conditional Proxy Re-Encryption

AUTHORS:J. Shao, G. Wei, Y. Ling, and M. Xie
This paper proposes a new cryptographic primitive, named identity-based conditional proxy re-encryption (IBCPRE). In this primitive, a proxy with some information (a.k.a. re-encryption key) is allowed to transform a subset of ciphertexts under an identity to other ciphertexts under another identity. Due to the specific transformation, IBCPRE is very useful in encrypted email forwarding. Furthermore, we propose a concrete IBCPRE scheme based on Boneh-Franklin identity-based encryption. The proposed IBCPRE scheme is secure against the chosen ciphertext and identity attack in the random oracle.

2) A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing

AUTHORS: Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Tran Viet Xuan Phuong, Qi Xie
In this paper, for the first time, we define a general notion for proxy re-encryption (PRE), which we call deterministic finite automata-based functional PRE (DFA-based FPRE). Meanwhile, we propose the first and concrete DFA-based FPRE system, which adapts to our new notion. In our scheme, a message is encrypted in a ciphertext associated with an arbitrary length index string, and a decryptor is legitimate if and only if a DFA associated with his/her secret key accepts the string. Furthermore, the above encryption is allowed to be transformed to another ciphertext associated with a new string by a semitrusted proxy to whom a re-encryption key is given. Nevertheless, the proxy cannot gain access to the underlying plaintext. This new primitive can increase the flexibility of users to delegate their decryption rights to others. We also prove it as fully chosen-ciphertext secure in the standard model.

3) An Efficient Cloud-based Revocable Identity-based Proxy Re-encryption Scheme for Public Clouds Data Sharing

AUTHORS:K. Liang, J. K. Liu, D. S. Wong, and W. Susilo
Identity-based encryption (IBE) eliminates the necessity of having a costly certificate verification process. However, revocation re-mains as a daunting task in terms of ciphertext update and key update phases. In this paper, we provide an affirmative solution to solve the efficiency problem incurred by revocation. We propose the first cloud-based revocable identity-based proxy re-encryption (CR-IB-PRE) scheme that supports user revocation but also a delegation of decryption rights. No matter a user is revoked or not, at the end of a given time period the cloud acting as a proxy will re-encrypt all ciphertexts of the user under the current time period to the next time period. If user is revoked in the forthcoming time period, he cannot decrypt the ciphertexts by using the expired private key anymore. Comparing to some naive solutions which require a private key generator (PKG) to interact with non-revoked users in each time period, the new scheme provides definite advantages in terms of communication and computation efficiency.

4)Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private

AUTHORS:Cécile Delerablée
This paper describes the first identity-based broadcast encryption scheme (IBBE) with constant size ciphertexts and private keys. In our scheme, the public key is of size linear in the maximal size *m* of the set of receivers, which is smaller than the number of possible users (identities) in the system. Compared with a recent broadcast encryption system introduced by Boneh, Gentry and Waters (BGW), our system has comparable properties, but with a better efficiency: the public key is shorter than in BGW. Moreover, the total number of possible users in the system does not have to be fixed in the setup.

5) Secure Identity Based Encryption Without Random Oracles
AUTHORS: D. Boneh and X. Boyen
We present a fully secure identity based encryption scheme whose proof of security does not rely on the random oracle heuristic. Security is based on the decisional bilinear Diffie-Hellman assumption. Previous constructions of this type incured a large penatly factor in the security reduction from the underlying complexity assumption. The security

reduction of the present system is polynomial in all the parameters.

III. METHODS AND MATERIAL

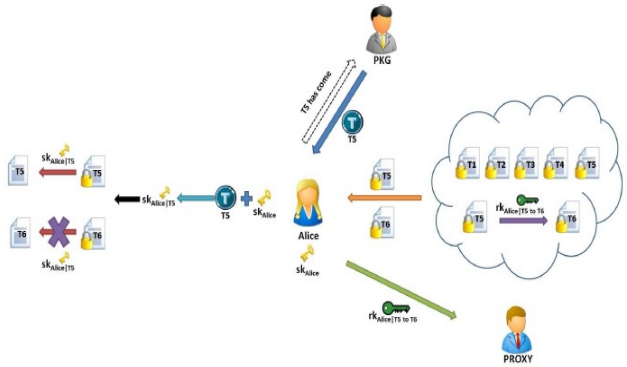

Figure 1: Architecture

In our proposed system, we use a trusted key generation Centre (KGC) which initializes the parameters used in our system and generates private keys for users of the application.A sender can encrypt his file by make use of receivers identities and file sharing conditions to securely share his files with multiple receivers.Furthermore, if sender likes to share some more files with other users which is having same condition, sender must delegate a re-encryption key specified with labeled having a condition to the proxy.Than that particular cipher-text is re-encrypted by proxy matching with the condition and the parameters to generate the re-encryption key is separate of the original receivers of that file.In our system not only initial authorized receivers can only access the file but also any new authorized user or any new registered user can also access the file by decrypting the re-encrypted cipher-text by make use of their private keys.

METHODOLOGY

Existing systems scheme sonly allows the re-encryption procedure is executed in an all- or-nothing manner. The proxy can either re-encrypt all the initial cipher texts or none of them. This coarse-gained control over cipher texts to be re-encrypted may limit the application of PRE systems. To fill this gap, are fined concept referred to as Proxy Double Encryption has been proposed. In this scheme a sender can enforce fine-grained re-encryption control over his initial cipher texts. The sender achieves this goal by associating a condition with a re- encryption key. Only the cipher texts meeting the specified condition can be re-encrypted by the proxy holding the corresponding re-encryption key. Are-encryption key tore-encrypt an initial cipher text, the sender needs to take the original receivers' identities of the initial cipher text as input. In practice, it means that the sender must locally remember the receivers' identities of all initial cipher texts. This requirement makes this scheme con-strained for the memory-limited or mobile senders and efficient only for special applications.

IV. RESULTS AND DISCUSSION

Figure 2 : File Encryption

Once the file is selected the encryption is done for security reasons .

Figure 3 : FileReencryption

Once the file is encrypted it is again re-encrypted ,if the same file is required by other users.

V. CONCLUSION

In our model we present a new kind of PRE concept called Secure Operations Of Cloud Email System By Using Contingent ID-Based Transmission Proxy Double-Encryption Technique, as well as its IND-Sid-CPA security definitions. Proposed system has general

concepts that include capabilities of all previous schemes such as conditional PRE, identity-based PRE and broadcast PRE. IND- Sid-CPA security definition of new system includes all the security requirements of CPRE, IPRE, and BPRE. This technique allows a user to share their outsourced encrypted data with other users in a Fine –grained manner. Our technique makes use of all user identities as public keys to encrypt the data. Which avoids a user to fetch and verify other user certificates before encrypting his data, as well as it allows a user to generate a broadcast cipher text that can be accessed by multiple receivers and share that encrypted data with multiple receivers in a batch manner.

VI. REFERENCES

[1]. J. Shao, G.Wei,Y.Ling, and M.Xie, "Identity-based conditional proxyre-encryption,"inProc.IEEEInt.Conf.Commun.,2011, pp.1–5.

[2]. MAN HO AU, JOSEPH K. LIU, WILLY SUSILO, DUNCAN S. WONG, GUOMIN YANG, TRAN VIET XUAN PHUONG, QI XIE, "A DFA- BASED

[3]. K.Liang,Z.Liu, X.Tan, D.S.Wong, and C.Tang, "ACCA-secure identity- based Conditional proxy re-encryption without random oracles," inProc.15thInt.Conf.Inf. SecurityCryptol.,2012, pp.231–146.

[4]. Cecile Delerablée "Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys"

[5]. D. BONEH AND X. BOYEN "SECURE IDENTITY BASED ENCRYPTION WITHOUT RANDOM ORACLES"