**Conditional Identity-Based Broadcast ProxyRe-Encryption and Its Application to Cloud Email**

**ABSTRACT:**

Recently, a number of extended Proxy Re-Encryptions (PRE), e.g. Conditional (CPRE), identity-based PRE (IPRE) andbroadcast PRE (BPRE), have been proposed for flexible applications. By incorporating CPRE, IPRE and BPRE, this paper proposes aversatile primitive referred to as conditional identity-based broadcast PRE (CIBPRE) and formalizes its semantic security. CIBPREallows a sender to encrypt a message to multiple receivers by specifying these receivers’ identities, and the sender can delegate are-encryption key to a proxy so that he can convert the initial ciphertext into a new one to a new set of intended receivers. Moreover, there-encryption key can be associated with a condition such that only the matching ciphertexts can be re-encrypted, which allows theoriginal sender to enforce access control over his remote ciphertexts in a fine-grained manner. We propose an efficient CIBPREscheme with provable security. In the instantiated scheme, the initial ciphertext, the re-encrypted ciphertext and the re-encryption keyare all in constant size, and the parameters to generate a re-encryption key are independent of the original receivers of any initialciphertext. Finally, we show an application of our CIBPRE to secure cloud email system advantageous over existing secure emailsystems based on Pretty Good Privacy protocol or identity-based encryption.

**EXISTING SYSTEM:**

* PRE and IPRE allows a single receiver. If there are morereceivers, the system needs to invoke PRE or IPRE multipletimes. To address this issue, the concept of broadcast PRE(BPRE) has been proposed. BPRE works in a similarway as PRE and IPRE but more versatile.
* In contrast, BPREallows a sender to generate an initial ciphertext to a receiverset, instead of a single receiver. Further, the sender can delegatea re-encryption key associated with another receiver setso that the proxy can re-encrypt to.
* A recent conditional proxy broadcast re-encryption scheme allows the senders to control the time to reencrypt their initial ciphertexts. When a sender generates a re-encryption key to re-encrypt an initial ciphertext, the sender needs to take the original receivers’ identities of the initial ciphertext as input. In practice, it means that the sender must locally remember the receivers’ identities of all initial ciphertexts. This requirement makes this scheme constrained for the memory-limited or mobile senders and efficient only for special applications.

**DISADVANTAGES OF EXISTING SYSTEM:**

* The early PRE was proposed in the traditional public-key infrastructure setting which incurs complicated certificate management.
* The PRE schemes only allow data sharing in a coarse-grained manner. That is, if the user delegates a reencryption key to the proxy, all ciphertexts can be reencrypted and then be accessible to the intended users; else none of the ciphertexts 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.
* No Identity provided for public keys to encrypt data.

**PROPOSED SYSTEM:**

* In this paper, we refine PRE by incorporating the advantagesof IPRE, CPRE and BPRE for more flexible applicationsand propose a new concept of conditional identitybasedbroadcast PRE (CIBPRE). In a CIBPRE system, atrusted key generation center (KGC) initializes the systemparameters of CIBPRE, and generates private keys forusers.
* To securely share files to multiple receivers, asender can encrypt the files with the receivers’ identitiesand file-sharing conditions. If later the sender would alsolike to share some files associated with the same conditionwith other receivers, the sender can delegate a re-encryptionkey labeled with the condition to the proxy,and the parameters to generate the re-encryption key isindependent of the original receivers of these files. Thenthe proxy can re-encrypt the initial ciphertexts matchingthe condition to the resulting receiver set.
* With CIBPRE,in addition to the initial authorized receivers who canaccess the file by decrypting the initial ciphertext withtheir private keys, the newly authorized receivers canalso access the file by decrypting the re-encrypted ciphertextwith their private keys.

**ADVANTAGES OF PROPOSED SYSTEM:**

* The sender does not need to download and re-encrypt repetitively, but delegates a single key matching condition to the proxy. These features make CIBPRE a versatile tool to secure remotely stored files, especially when there are different receivers to share the files as time passes.
* We define a practical security notion for CIBPRE systems. Intuitively, without the corresponding private keys, one can learn nothing about the plaintext hidden in the initial or re-encrypted CIBPRE ciphertext; an initial ciphertextcan not be correctly re-encrypted by a re-encryption key if the ciphertext and the key are associated with different conditions.
* We propose an efficient CIBPRE that is provably secure in the above adversary model. We prove that the IND-sIDCPA security of the proposed CIBPRE scheme if the underlying identity-based broadcast encryption (IBBE) scheme is secure and the Decisional Bilinear Diffie-Hellman (DBDH) assumption holds. Our proposed CIBPRE scheme enjoys constant-size initial and re-encrypted ciphertexts, and eliminates the constraints of the recent work

**SYSTEM ARCHITECTURE:**



**MODULES:**

* System Construction Module
* Proxy Re-encryption Module
* Trusted Key Generation Center (KGC)
* Cloud Email

**MODULES DESCRIPTION:**

**System Construction Module:**

* In this module a user can upload and send datas to other users in cloud mail and other users can recive the data in cloud mail with a secure way. CIBPRE system, an trusted key generation center (KGC) initializes the system parameters of CIBPRE, and generates private keys for users.
* A sender can encrypt the files with the receivers’ identities and file-sharing conditions. If later the sender would also like to share some files associated with the same condition with other receivers, the sender can delegate a reencryption key labeled with the condition to the proxy, and the parameters to generate the re-encryption key is independent of the original receivers of these files. Then the proxy can re-encrypt the initial ciphertexts matching the condition to the resulting receiver set. With CIBPRE, in addition to the initial authorized receivers who can access the file by decrypting the initial ciphertext with their private keys, the newly authorizedreceiverscanalso access the file by decrypting the re-encrypted ciphertext with their private keys. Note that the initial ciphertexts may be stored remotely while keeping secret.
* The sender does not need to download and re-encrypt repetitively, but delegates a singlekeymatchingconditiontothe proxy.

**Proxy Re-encryption Module:**

* In Proxy re-encryption a User may encrypt his file with his own public key and then store the ciphertext in an honest-but-curious server. When the receiver is decided, the sender can delegate a re-encryption key associated with the receiver to the server as a proxy.
* Then the proxy re-encrypts the initial ciphertext to the intended receiver. Finally, the receiver can decrypt the resulting ciphertext 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, and (2) before receiving the
re-encryption key, the proxy can not re-encrypt the initial ciphertext in a meaningful way.

**Trusted Key Generation Center (KGC):**

* In this moduleKey generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted by user.The trusted key generation is used for initializes the system parameters of CIBPRE, and generates private keys for users.
* The KGC generates the system parameters to initialize the CIBPRE based cloud email system. It chooses a security parameter 2 N and a value N 2 N (the maximal number of receivers of an email), and runs algorithm SetupPREð NÞ to generate a pair of master public and secret keys PKPRE and MKPRE. It chooses a secure symmetric key encryption scheme.
* When a new user joins this system, the KGC generates a private key for him. Without loss of generality, let ID denote the email address of the new user. The KGC runs algorithmExtract to generate the private key SKPRE ID ,and sends it to the user in a secure channel which is established by the SSL/TLS protocol.

**Cloud Email:**

* In this module CIBPRE-based cloud email system, the enterprise administrator only needs to initialize the system and generate the private key for the newly joined user. In other words, the enterprise administrator can be offline if no new user joins the system. It is a useful paradigm for the enterprise administrator to resist the outside attacks in practice.
* It is a useful paradigm for the enterprise administrator to resist the outside attacks in practice. Thecloud server provides efficient services to send, store and forward users’ encrypted emails. Moreover, it is convenient that all users take email addresses as public keys to encrypt emails. In the aspect of security, all users’ emails are confidentialeven if the cloud sever is compromised.
* A user can send an encrypted email to other users. And 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. Suppose user ID1 wants to send the email content F (including the associated attachment) to the users.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL

**REFERENCE:**

PengXu, Member, IEEE, Tengfei Jiao, Qianhong Wu, Member, IEEE,Wei Wang, Member, IEEE, and Hai Jin, Senior Member, IEEE, “Conditional Identity-Based Broadcast ProxyRe-Encryption and Its Application to Cloud Email”, **IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 1, JANUARY 2016.**