Contingent Identity-Based Broadcast Proxy Re-Encryption and its Application to Cloud Email

Dr. Dhananjay M[1] Asma Farheen[2]
[1]Assistant Professor [2]M. Tech. Student
[1,2]Department of Computer Science & Engineering
[1,2]GNDEC, Bidar, Karnataka, India

Abstract— As of late, various expanded Proxy Re-Encryptions (PRE), e.g. Contingent (CPRE), identity based PRE (IPRE) and broadcast PRE (BPRE), has been proposed for adaptable applications. By consolidating CPRE, IPRE and BPRE, this paper proposes a flexible primitive alluded to as contingent identity- based broadcast PRE (CIBPRE) and formalizes its semantic security. CIBPRE enables a sender to scramble a message to various beneficiaries by indicating these recipients' personalities, and the sender can delegate to a re-encryption key to a proxy with the goal that he can change over the underlying cipher text into another to a new set of intended receivers. Additionally, 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 CIBPRE plot with provable security. In the instantiated conspire, the underlying cipher text, the re-encoded cipher text and the re-encryption enter are all in steady size, and the parameters to create a re-encryption key are autonomous of the first beneficiaries of any underlying cipher text. At long last, we demonstrate a utilization of our CIBPRE to secure cloud email framework worthwhile over existing secure email frameworks in light of Pretty Good Privacy convention or character based encryption.

Key words: Proxy Re-Encryption, Cloud Storage, Identity-Based Encryption, Broadcast Encryption, Cloud Email

I. INTRODUCTION

PROXY re-encryption (PRE) 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

- Neither the server/proxy nor non-intended receivers can learn any useful information about the re-encrypted file, nor
- Before receiving the re-encryption key, the proxy cannot re-encrypt the initial cipher text in a meaningful way.

II. LITERATURE SURVEY

In [1] J. Shao, G. Wei, Y. Ling, and M. Xie the authors of this paper proposes a new cryptographic primordial, named identity-based conditional proxy re-encryption (IBCPRE). Here, a proxy has given with some information (a.k.a. re-encryption key) is allowed to transform a subset of cipher texts under an identity to other cipher texts under another identity. Due to the specific feature of transformation, the above technique is very helpful in encrypted email forwarding. Moreover, we also build a detailed IBCPRE scheme based on Boneh-Franklin identity-based encryption. The developed IBCPRE scheme is secure against the chosen cipher text and identity attack in the random oracle.

In [2]Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Tran Viet Xuan Phuong, Qi Xie: here in this paper, we develop a general notion for proxy re-encryption (PRE), which is known to be deterministic finite automata-based functional PRE (DFA-based FPRE). Further, we also build the first and concrete DFA-based FPRE system, which suit to our new state. In our proposed model, the available data is encrypted in a cipher-text along with an arbitrary length index string, and a descriptor is applicable if and only if a DFA along with his/her secret key accepts the string, Moreover the given encryption is allowed to be transformed to another cipher-text associated with a new string by a semi-trusted proxy to whom a re-encryption key is given. As a proxy will not get access to the private plaintext. This new feature can increase the flexibility of users to delegate their decryption rights to others. Hence we prove that it is a fully chosen-cipher text secure in the accepted model.

In [3]K. Liang, J. K. Liu, D. S. Wong, and W. Susilo Identity-based encryption (IBE) removes the requirement of carrying a costly certificate verification process. whereas, revocation remains as a horrifying task in terms of initial cipher text as well as key update phases.to explain the efficiency problem obtain by revocation we develop this particular scheme. Here, in this scheme we develop the first cloud-based revocable identity-based proxy re-encryption (CR-IB-PRE) scheme which supports a user revocation as well as consignment of the decryption rights. the particular cloud which is assigned as a proxy will re-encrypt all the available cipher-text provided by the user in between the current time to the next time period, as it is none bother whether the user is renounce or not. Suppose if we call the user in the upcoming period, he is just unable to decrypt the available data by using the lapsed private keys in previous schemes which needs a private key generator(PKG)to interact with non-revoked users in each time period, hence our proposed scheme provides definitive advantages in terms of communication and computation.

In [4]Cécile Delerablée: here in this particular scheme we define the first ever identity-based broadcast encryption scheme (IBBE) which may have a constant size cipher-text as well as it may have various private keys.

Here, in our scheme we have a public key of linear size, and a set of receivers of maximal size m, which is basically smaller than the number of users/identities in a system. If we compare our scheme with a recent broadcast

encryption system which was introduced by Boneh, Gentry and waters(BGW), our scheme has comparable properties as well as our proposed system has a better efficiency(in terms of the public key is shorter in(BGW)).And the number of possible users using the system requirements is not fixed.

In [5]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 incurred a large penalty factor in the security reduction from the underlying complexity assumption. The security reduction of the present system is polynomial in all the parameters.

III. SYSTEM ARCHITECTURE

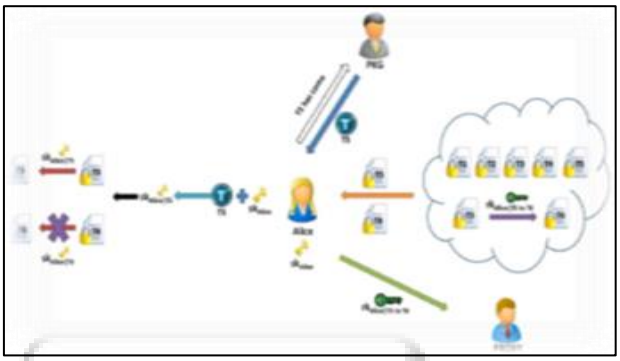

Fig. 1: System Architecture

- 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.

IV. MODULE DESCRIPTION

A. *Proxy Re-encryption Module*

- In this particular module a user can encrypt his data file by make use of his public key. After encrypting the file we store the resulting re-encrypted data in an honest but curious server. Once the receiver is decided for data sharing the sender can delegate a re-encryption key associated with the receiver to the server as a proxy.
- Then that particular proxy re-encrypts the initial cipher-text for the requested receiver set.
- Lastly, the receiver will decrypt the resulting cipher-text by make use of his private keys.

PRE usually reassures in terms of security as

1) Not either the server/proxy nor non-intended receivers can able to learn any useful information regarding re-encrypted file, and moreover
2) Without receiving the re-encryption key, the proxy is unable to re-encrypt the initial cipher-text in a useful way.

B. *System Construction Module*

Here, each user can upload and send files to other users in cloud mail and other users of the system can receive the data in cloud mail with a protected way. In our scheme a trusted key generation center (KGC) load system parameters and produces private keys for all the users of the system. Sender of data can encrypt the files with the receiver's identities and specified file sharing condition with the receiver's, the sender will delegate a re-encryption key along with the labeled condition to the proxy and the number of parameters required to develop the re-encryption key is separate of the receivers of the files. Further proxy can re-encrypt the initial cipher-text matched the specific conditions to the receivers

C. *Cloud Email*

Here we use a cloud email system for our CIBPRE module, in this the enterprise administrator just need to start the system and develop the private keys for individual new joined user. This means if there is no new user to join the system, the administrator remains offline. This is a special character of enterprise administrator to resist the attacks. We have a cloud server which provides efficient services to send the encrypted email data, to store that data, and to forward the data. Also it is very convenient that all the users of the system take the email addresses as their public key for encryption. Security will be maintained, as all user emails are confidential. Here a user will send the encrypted email to other user, which is stored in a cloud server. If a user wants to read this email he can decrypt it by fetching from cloud server.

D. *Trusted Key Generation Center (KGC)*

A process by which we generate keys in cryptography is known to be a key generation process. We use key for the purpose of encryption or decryption of the user data.

We are using a trusted key generation for initializing the system parameters of CIBPRE and generate private keys for each registered user. We make use of KGC to generate system parameters to load the CIBPRE based email environment it make use of a security parameter 2N and a value N2N (the maximum number of email receivers) it also runs an algorithm setup PRE to generate a pair of master public and secret keys PKPRE and MKPRE. It adopts a secure symmetric key encryption scheme for key generation. If a new user joins the system, without losing its generality KGC will generate private keys for them. Let's take an example here ID denote users email address, to generate private key for new user KGC runs an algorithm which generate key SKPRE ID, and it will send it to the intended user in a secure channel which is developed using SSL/TLS protocol.

V. RESULTS

A. Home Page

Fig. 2: Home page

B. Registration Page

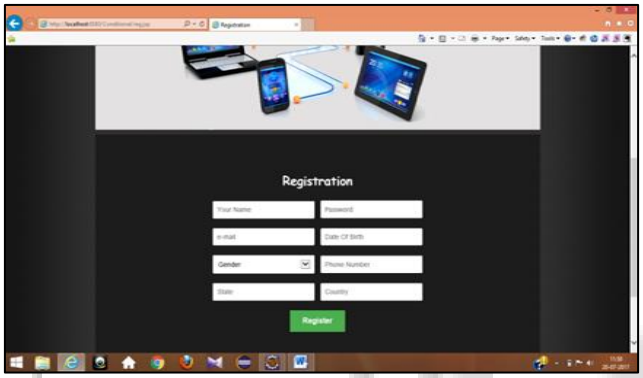

Fig 3. Registration Page

C. User Login

Once the registration is done, the user can login by providing the user credentials.

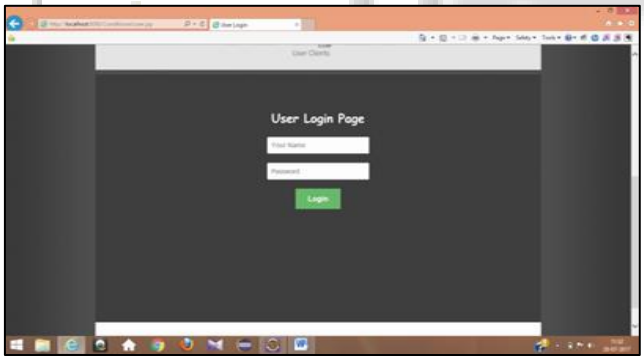

Fig. 4: User Login Page

D. File selection for Encryption

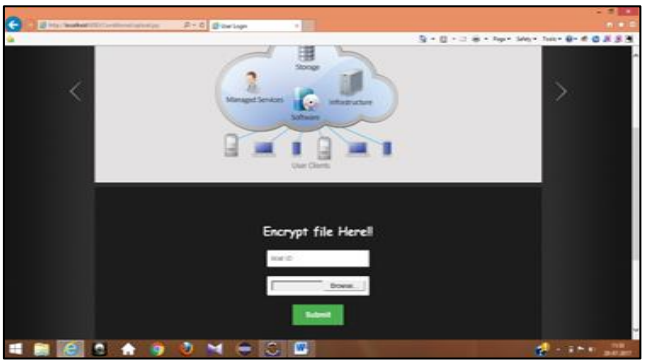

Fig. 6: File selection page

Here the user selects the file that need to be encrypted for security purpose.

E. File Encryption

Once the file is selected the encryption is done

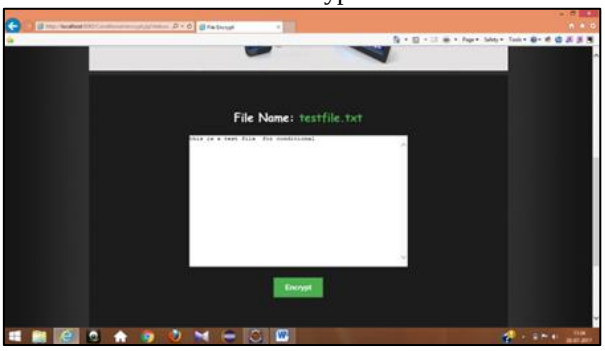

Fig. 7: Encryption Page

F. File Re-encryption

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

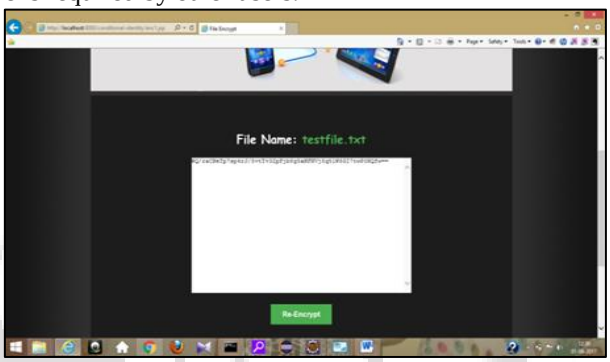

Fig. 8: File Re-encryption

G. File Download

When the user wants to download a file the file will be encrypted format.

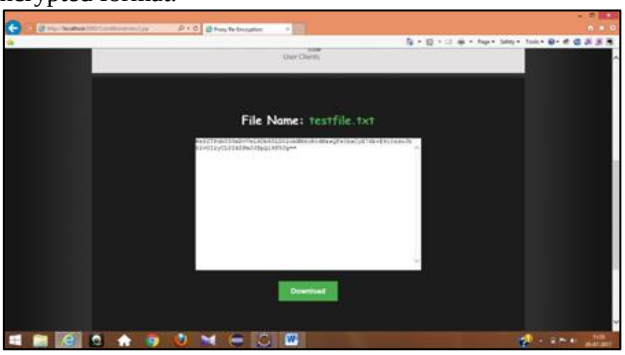

Fig. 9: File Download

H. File Request

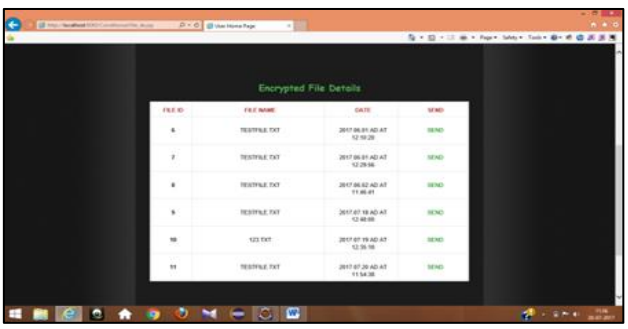

Fig. 10: File Request

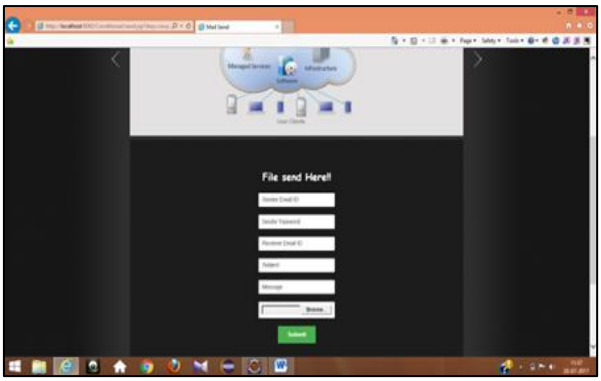

Fig. 11: File sent

When the receiver wants to download a file, the response for the request is provided by the user. The receiver details need to be provided along with receiver public key and submitted.

I. File Decryption and RE-decryption

Once the encrypted file is received, it is decrypted and re-decrypted by using file id and secret key which is known only to the user.

Fig. 12: File selected

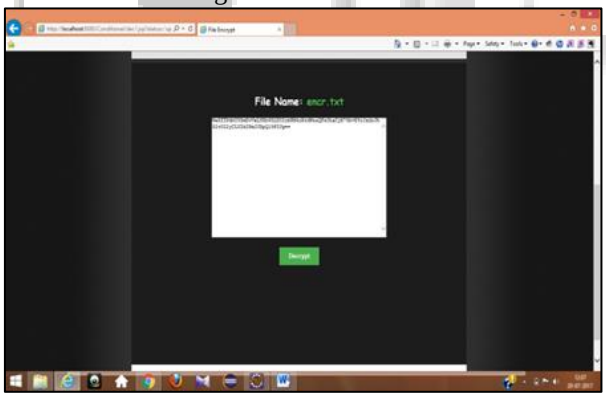

Fig. 13: File Decryption

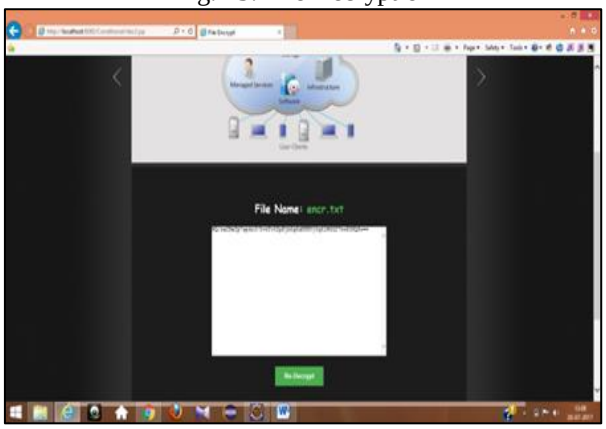

Fig. 14: File Re-Decryption

J. Final Download

Once the decryption is done, the normal file is available to the receiver.

Fig. 15: Normal File

K. Cloud Login

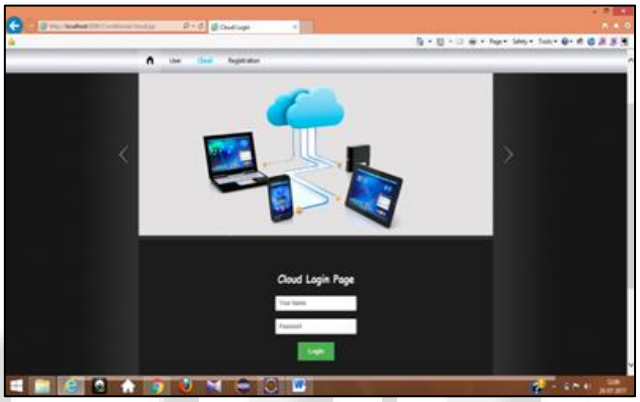

Fig. 16: Cloud Login

VI. CONCLUSION

In this paper, a new kind of PRE concept called contingent-identity based broadcast proxy re-encryption (CIBPRE), as well as its IND-sID-CPA security definitions. CIBPRE has general concepts that include capabilities of all previous schemes such as conditional PRE, identity-based PRE and broadcast PRE. S IND-Sid-CPA security definition of CIBPRE 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. This 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. We implemented the first CIBPRE scheme that is based on identity-based broadcast encryption by using provable security of the IBBE scheme and the DBDH assumption. This indicates that without using private key or without the right to share users outsourced data one can learn nothing about the user's data.

ACKNOWLEDGMENTS

We are indebted to the management of GNDEC, Bidar, for excellent support in completing this work at the right time. A special thanks to the authors mentioned in the references.

REFERENCES

[1] 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.
[2] K. Liang, M. H. Au, J. K. Liu, X. Qi, W. Susilo, X. P. Tran, D. S. Wong, and G. Yang, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.
[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. Eur. Symp. Res. Comput. Security, 2014, pp. 257–272.
[4] Delerablee, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in Proc. 13th Int. Conf. Theory Appl. Cryptol. Inf. Security: Adv. Cryptol., 2007, pp. 200–2015.
[5] D. Boneh and X. Boyen, "Efficient selective-id secure identity based Encryption without random oracles," in Proc. Adv. Cryptol., 2004, pp. 223–238.

