File Encryption By Using Short Ciphertexts

Bhavya Devadiga [1], Dr. Surendra Shetty[2]
[1, 2] Dept of Master of Computer Application
[1, 2] NMAM Institute of Technology, Nitte
Udupi, Karnataka, India.

Abstract- *In "File Encryption by using short Ciphertexts" which allows the sender to broadcast any subset members but may require a trusted third party to securely distribute decryption keys. The group key agreement protocol which gives an authority to group of members to bring out a common encryption key in an open network so that the group members can only decrypt the cipher texts that is being encrypted under the shared encryption keys, but the sender cannot deny any particular member from decoding the cipher texts. In this work, we combine these two notations to form a contributory broadcast encryption. In this we relate a group of members to bring out a common public encryption key while each of the member will hold a decryption key. A sender by seeing this public group encryption can restrict the decryption a part of a member of his choice. By this, we propose this application.*

I. INTRODUCTION

1.1 Project Introduction

The "**File Encryption by using short Ciphertexts**" application which is mainly developed for enabling security to group of users and individual users. This application is fast and advanced developing communication technologies.

This software application provides security to owners and users from the scratch by generating secret key. The key can be generated once the users registers to the application. Therefore, the users or group of users can access the file from the cloud if the users are authorized to access the cloud. If the cloud accepts a particular user to download a file then a secret key and a one-time password is received by the user using mail. As well as if the cloud accepts the owner then a secret key for sending any file is received by the owners using mail.

1.2 Problem Description

"**File Encryption by using short Ciphertexts**" is online application which mainly developed for providing security for sending data like pdf, images, document etc. This application generates secret key for individual user and to group of users. It may allow to access all the members in the group while downloading the file from the cloud. While providing secret key to group of users each group member will not be able to get different secret keys. Accessing the file from the cloud is time

II. LITERATURE SURVEY

Literature survey is the most important in software development process. Before the developing tool it is most important to determine that time factor, economy and company strength takes a major role. Once these things are contented, then the next step is to determine which operating system and language can be used for developing the tool. Then once the programmers start building the tool the programmers need lot of external support. This support can be obtained from, websites, books and senior programmers.

Broadcast encryption

Broadcast Encryption enables to distribute keys in a secure way for sender and the receiver. In this work, we mainly use Id [1] based encryption scheme that can distribute the keys all over in an open network. So that this may help each subset of user to recognize a specified key. By using DES [1], which will encrypt the distributed key. A key distribution can be done by using pre distribution and also by using re keying protocol for accessing group members operation which can be simplified. By using Id based encryption technology, can be used to distribute new keys.

A conference key distribution system

In this encryption, which is mainly used to have a secure information or data to send from anyone other than the third party users. To make use of this encryption and decryption technique, these sender and receiver thought to have a same keys during the key distribution. But however it can take only one pair at a time to share keys towards the encryption and decryption [1].By using some of the public keys can have conference in a key distribution. We mainly use CKDS [2] in this distribution.

"Key agreement in dynamic peer groups"

In this technique, by using the group key this may result in increased group based oriented application and by

using protocol also by using communication in group which will occur in many backgrounds. Key agreement in background is the first step in reliable services. All the agreement of group key [6] operations and we use a Cliques [5] which will give agreement group key services.

III. SYSTEM STUDY

3.1 Existing System with Limitations

In cryptography, there is no security for group oriented communication. A key agreement standard which allows a same key for all the members in the group. Each member in a group may not have a different keys. To overcome this, a common public key is used, and each group member will hold different decryption key. But this is symmetric.

This needs a trusted third party so that cannot handle sender or member that changes successfully.

IV. PROPOSED SYSTEM WITH OBJECTIVES

We use the **File Encryption by using short Ciphertexts** primitive, which is the combination of group key agreement and broadcast encryption. In this work, we illustrate the necessity of the group oriented communication and also security to the users of the disclosed broadcast encryption building block and show the feasibility of our contributory broadcast encryption scheme with experiments which provides complete safety proofs.

We produce a different secret keys for each member in a group. So that each member in group can decrypt any given file. Also for individual users can also decrypt the file that by using the given secret key.

The main objective of this software is to provide security in order to avoid from the attackers. Finally, we construct a well-organized contributory broadcast encryption scheme with our broadcast encryption systematic plan as a building block.

V. METHOD

Depending on the implementation, only a registered member either an owner or user can be able to access. Once the user or an owner is registered, then it must wait until the cloud activates. Once the cloud activates, then the owner can upload the file by using the secret key.

User gets a secret key in order to login. But the user can download the file directly until the request sent to the cloud activates. Once activated the user gets a secret key and a one-time password in order to decrypt a file.

VI. CONCLUSION

Anyone can send secret messages to any of the group members, and the system does not require a trusted key server. An efficient Contributory broadcast encryption scheme that is secure in the standard model. A new path is created to broadcast channels securely in a numerous way in a distributed application.

REFERENCES

[1] A. Fiat and M. Naor, “Broadcast Encryption,” in Proc. Crypto 1993, 1993, vol. LNCS 773, Lecture Notes in Computer Science, pp. 480-491.

[2] I. Ingemarsson, D.T. Tang and C.K. Wong, “A Conference Key Distribution System,” IEEE Transactions on Information Theory, vol. 28, no. 5, pp. 714-720, 1982.

[3] Q. Wu, Y. Mu, W. Susilo, B. Qin and J. DomingoFerrer, “Asymmetric Group Key Agreement,” in Proc. Eurocrypt 2009, 2009, vol. LNCS 5479, Lecture Notes in Computer Science, pp. 153-170.

[4] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farr`as, “Bridging Broadcast Encryption and Group Key Agreement,” in Proc. Asiacrypt 2011, 2011, vol. LNCS 7073, Lecture Notes in Computer Science, pp. 143-160.

[5] Michael Steiner, Gene Tsudik, Member, IEEE Computer Society, and Michael Waidner, Member, IEEE Computer Society, “Key Agreement in Dynamic Peer Groups”, IEEE Transactions on parallel and distributed systems, VOL. 11, NO. 8, August 2000.

[6] Qianhong Wu, Member, IEEE, Bo Qin, Lei Zhang, Member, IEEE, Josep Domingo-Ferrer, Fellow, IEEE, Oriol Farras, and Jesus A. Manjon, “Contributory Broadcast Encryption with Efficient Encryption and Short Ciphertexts”, IEEE Transactions on computers, VOL. 65, NO. 2, February 2016.