© 2016 IJSRST | Volume 2 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

An Efficient Group Key Agreement Protocol for Online Social Network

Sowmya. R, R. Gowri, D. Hemavathy

Department of Computer Science and Engineering, Dhanalakshmi College of Engineeering, Chennai, Tamil Nadu, India

ABSTRACT

The objective of this project is to study a group key agreement problem where a user is only aware of his neighbors while the connectivity graph is arbitrary. In our problem, there is no centralized initialization for users. A group key agreement with these features is very suitable for social networks. Under our setting, we construct two efficient protocols with passive security. We obtain lower bounds on the round complexity for this type of protocols, which demonstrate that our constructions are rounding efficient. Finally, we construct an actively secure protocol from a passively secure one.

Keywords: Data Sharing, Data Privacy, Diffie Hellman, Lower Bound.

I. INTRODUCTION

Key agreement is a mechanism that allows two or more user two share a secret key in a secure manner. Almost, all the protocols assume a whole connectivity graph which means any two users can communicate directly. In, any social network a post or commend can be communal publicly. Even if it is shared privately it can be accessed by the mutual friends. There is no secret sharing of information between two users. So to make a secure transmission of information between two users, we use RSA algorithm. Using this algorithm we encrypt and decrypt the data files. The user can transmit the data files with the help of private key and group key. Both the keys are used to transmit the information in a more secured form.

Related Works

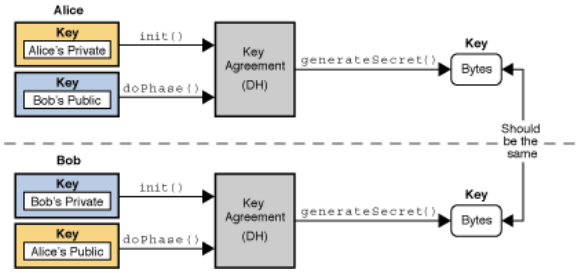
A rekey scheme can be defined as a centralized dynamic broad cast encryption, where the authority maintains the group and updates the group key. The drawback of this system is that the user key will be updated whenever the group changes. So we cannot adopt a rekeying scheme as a group key agreement. In the previous work, in any social network the information can be shared publicly. Even if it is shared a private key it can be read by the mutual friends and users. Key pre distribution system is a non-interactive group key agreement. In this case the shared key of a given group is fixed. The drawback of KPS is that if the number of user increases then the key size also increase. Another drawback is that group key of a given group cannot be changed even if it is leaked. Traitor tracing is a special type of broad cast encryption which can trace the pirate user. If the user builds an illegal decryption device, it will be identified. It has the drawbacks of broadcast encryption.

II. METHODS AND MATERIAL

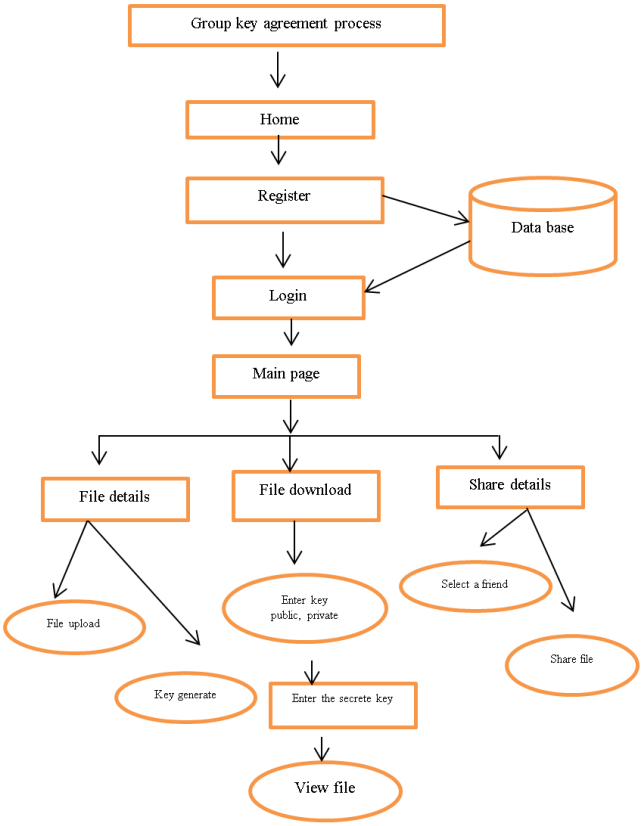
The project is proposed to make a protected transmission of information in social networks between the users. The group key and private key provide security. While, the user needs to transmit secret information to a particular user, the user can transmit it with the help of private key and group key. Since, the group key is publicly available; the user with correct matching key with the transmitted private key can only decrypt the information. The public key can be created using RSA algorithm for encryption and the private key can be created using attribute based system for decryption. Thus everyone else is denied to

access the information. So this system is more secured when compared to existing methodologies.

Architecture Diagram



Data Flow Diagram



Attribute Based Encryption:

Attribute-based encryption is a kind of public-key encryption in which the secret key of a user and the ciphertext are reliant on upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is likely only if the set of attributes of the user key matches the attributes of the ciphertext. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds several keys should only be able to access data if at least one individual key grants access.

- Setup. A randomized algorithm Setup(k) takes in as input a security parameter and provides a set of public parameters (PK) and the master key ideals (MK).
- Encryption. The algorithm Enc(M, T , PK) is a randomized algorithm that proceeds as input the message to be encrypted (M), the entrée structure T which needs to be satisfied and the public parameters (PK) to output the ciphertext CT. We can say, that the encryption system embeds the access structure in the ciphertext such that only those users with attributes satisfying T will be able to decrypt and retrieve the message M.
- Key-Generation. The KeyGen(MK, PK, A) algorithm proceeds as input the master key values (MK), the public parameters (PK) and the attribute set of the user (A), and yields for the user a set of decryption keys SK which confirms the users possession of all the attributes in A and no other external attribute.
- Decryption. The decryption algorithm Dec(CT, SK, PK) takes as input the ciphertext CT, the user secret keys SK and the public bounds PK, and it outputs the encrypted message (M) if and only if the attributes A embedded in SK satisfy the access structure T which was used while encrypting the ciphertext CT. i.e If T (A) = 1 then message M is output else, it outputs.

RSA Algorithm:

The RSA algorithm involves a public key and a private key. The public key is used for encrypting message. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The basic principle of RSA is to find three large positive integers *e*, *d* and *n* such that the modular exponentiation for all *m.*

$(m^e)^d \bmod n = m$

Additionally this relation also implies for some operation is convenient,

$(m^d)^e \bmod n = m$

1. Group Key Agreement:

The group key agreement with an arbitrary connectivity graph, where each user is only aware of his neighbors

and has no information about the existence of other users. Further, he has no information about the network topology. Under this setting, a user does not need to trust a user who is not his neighbor. Thus, if one is initialized using PKI, then he need not trust or remember public-keys of users beyond his neighbors.

2. Key pre-distribution system (KPS):

In this case, the shared key of a given group is fixed after the setup. If a group is updated, then the group key changes to the shared key of the new group. Further, computationally secure KPS is only known for the two-party case and the three-party case. KPS with a group size greater than 3 is still open.

3. Lower Bound:

Broadcast encryption is a mechanism that allows a sender to send a group key to a selected set of users. In a symmetric key based broadcast encryption, the sender is a fixed authority. In this case, the user key size is combinatorial lower bounded. In addition, it is secure only against a limited number of users. In a public key broadcast encryption, the key size problem can be waived. The cipher text size depends on the number of users and hence could be large (e.g., it is O (p n) in for n users). Under our setting, we construct two efficient passively secure protocols. We also prove lower bounds on the round complexity which demonstrates that our protocols are round efficient. Finally, we construct an actively secure protocol from a passively secure one.

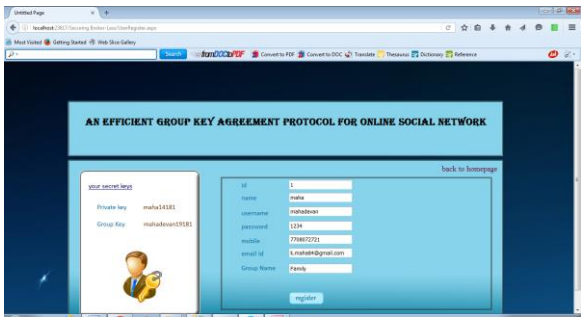
4. Diffie-Hellman protocol:

The computationally secure group key agreement in a passive model. This started from the Diffie-Hellman protocol. In the following, we use the tuple (a; b; c) to represent a protocol that has a rounds, b elements of messages per user (the unit is a field element in Z_ p for a large prime p) and computation cost c. designed a group key agreement for n users in a ring with an efficiency tuple Their protocol assumes a complete connectivity graph. The proposed protocols in the random oracle model, where the interesting construction has an efficiency tuple.

III. RESULT AND DISCUSSION

Registration

We are creating a website and sign up the page for registration. And the register page is viewed then filled our details and submits the registration. Then the server generates the group key and private key.



Main Page

We are creating the user name and password by using the registration. The user can login through their username and password. After the login main page will appeared.

The main page contains the view member page, file upload, share file and file download. It is based on the user opinion to access the file (ie. Upload and sharing).

Download

To download a file we must need a private key and public key. Key was checked by the server. If the key is not matched we cannot download the file.

IV. CONCLUSION

We studied a group key problem where there is a secured transmission of information between the users. It is very suitable for applications such as social networks like facebook. In facebook the post or messages can be accessed by mutual friends. So, secrete sharing of information between user is not possible. In this project we create a private key for each user in this group. we construct two efficient protocols with passive security. So it maintains secure relationships between the users.

V. REFERENCES

[1] T. M. Cover and J. A. Thomas, Elements of Information Theory, Wiley, New York, 2006.

[2] D. Boneh, A. Sahai and B. Waters, "Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys", Proc.25th Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT'06) , vol. 4004, pp. 573-592, 2006.

[3] R. Dutta and R. Barua, "Provably Secure Constant Round Contributory Group Key Agreement in Dynamic Setting", IEEE Trans. Information Theory, vol. 54, no. 5, pp. 2007-2025, 2008.

[4] D.Boneh and M.Naor,"Traitor tracing with constant size ciphertext",Proc. 15th ACM Conf. computer and comm. Security, pp.501-510,2008.

[5] R.Safavi-Naini, S.Jiang, "Non-intractive Conference Key Distribution and Its Application", Proc. The 2008 ACMA symposium on Information, Computer and Communication Security (ASIACCS'08), pp.271-282, 2008

[6] Q.Wu,Y.Mu,W.Susilo,B.Qin and J. Domingo-Ferrer," Asymmetric group key agreement",Proc.28 Int'l Conf. Theory and application of cryptographic techniques (EUROCRYPT'09), vol.5479,pp. 153-170,2009.

[7] R.Safavi-Naini, S.Jiang, "Unconditionally Secure Conference Key Distribution: Security Notions, Bounds and Constructions", International Journal of Foundations of Computer Science, vol.22, no.6, pp.1369-1393, 2011.

[8] X.Lv,H.Li and B.Wang, "Group Key agreement for secure group communication in dynamic peer systems", J.Parallel Distrib. comput., vol.72, no.10,pp.1195-1200,2012.