International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

Group Key Agreement Efficient In Communication

[1] N Vasavi Reddy [2] G Karunakar Goud, [3] Prasad B
[1]II/IV, [2][3]Associate Professor
[1][2][3] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM) Hyderabad
[1] vasavireddy27@gmail.com [2] karna3009@mlritm.ac.in [3]bprasad@gmail.com

Abstract :-Key agreement is a mechanism that allows two or more parties to securely share a secret key (called a session key). Starting from Diffie-Hellman for the two-party case. However, almost all the protocols assume a complete connectivity graph: any two users can communicate directly. In the real world, this is not always true. For instance, in social networks such as Face book, Skype, Wechat and Google+, a user is only connected with his friends. For a group of users (e.g., the faculty union in a university) who wish to establish a session key, it is not necessary that any two of them are friends. But they might still be connected indirectly through the friend network. Of course, we can still regard them as directly connected by regarding the intermediate users as routers. However, this is quite different from a direct connection. First, indirectly connected users may not have the public information of each other (e.g., public-key certificate). Second, indirectly connected users may not know the existence of each other (e.g., in our faculty union example, one professor in one department may not know another professor in a different department). Third, a message between two indirectly connected users travels a longer time than that between directly connected users. We study 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.

***Keywords*: Diffie-Hellman, Secret Key, Session Key, Pre-Distribution System.**

I. INTRODUCTION

Aim:
The aim of this paper is study a group key agreement problem where a user is only aware of his neighbors while the connectivity graph is arbitrary.

Scope:
The Scope of this paper is to construct an actively secure protocol from a passively secure one.

Existing System:
Key pre-distribution system (KPS) (a.k.a. non-interactive conference distribution system) can be regarded as a non-interactive group key agreement. 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. The drawback of KPS is that the user key size is combinatorial large in the total number of users (if the system is unconditionally secure). Another drawback is that the group key of a given group cannot be changed even if it is leaked unexpectedly (e.g., cryptanalysis of cipher texts bearing this key). The key size problem may be overcome if a computationally secure system is used, while the key leakage problem is not easy. 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.

Disadvantages Existing System:
The user key size is combinatorial large in the total number of users (if the system is unconditionally secure).
The group key of a given group can not be changed even if it is leaked unexpectedly.

Proposed System:
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.

Advantages Proposed System:
To update the group key more efficiently than just running the protocol again, when user memberships are changing.
Two passively secure protocols with contributiveness and proved lower bounds on a round complexity, demonstrating that our protocols are round efficient.

II. DESIGN

A. Architecture:

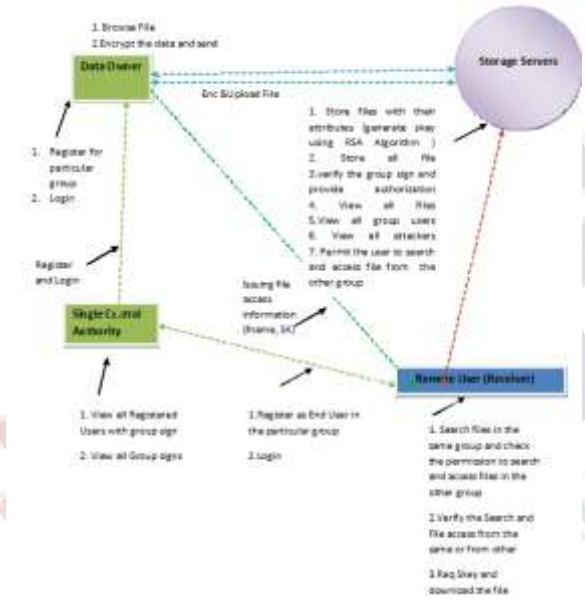

Fig 1: System Architecture

B. Data Flow Diagrams:

Level - 0:

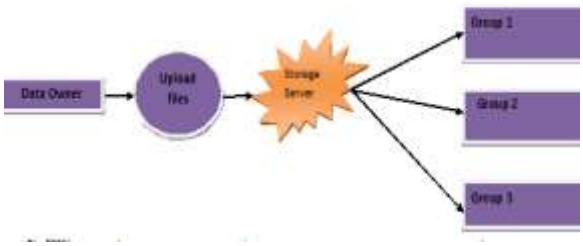

Fig 2: Level – 0 Data Flow Diagrams

Level - 1:

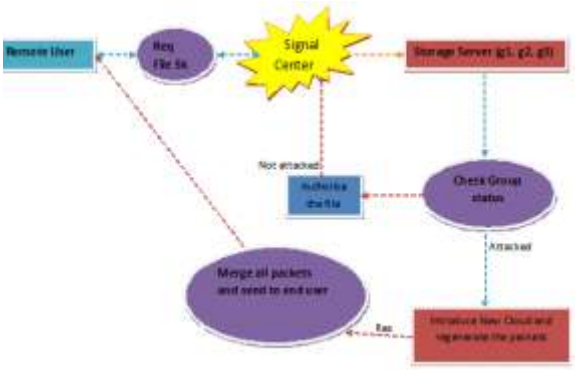

Fig 2: Level – 1 Data Flow Diagrams

C. Modules

The modules involved in the system are Data Owner(Group Member), Web Storage Server , Single Central Authority, Data Integrity and Data Consumer(End User / Group Member).

Data Owner (Group Member):
In this module, the data owner uploads their data in the web server. For the security purpose the data owner encrypts the data file and then store in the web . The Data owner can have capable of manipulating the encrypted data file.

Web Storage Server:
The web service provider manages a web to provide data storage service. Data owners encrypt their data files and store them in the web for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the web and then decrypt them.

Single Central Authority:
The Single Central Authority manages all data forwards to web service provider and if there is any un matching key then it will sent to public Verifier to revoke the user details and performs the following operations such as View all Registered Users with group sign, View all Group signs.

Data Integrity:
Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

Data Consumer (End User / Group Member):
In this module, the user can only access the data file with the encrypted combined key if the user has the

privilege to access the file and perform the following operations Search files in the same group and check the permission to search and access files in the other group, Verify the Search and File access from the same or from other ,Req Skey and download the file.

III. IMPLEMENTATION

Fig 1: Login Page

Fig 2: Owner Login

Fig 3: Owner Details

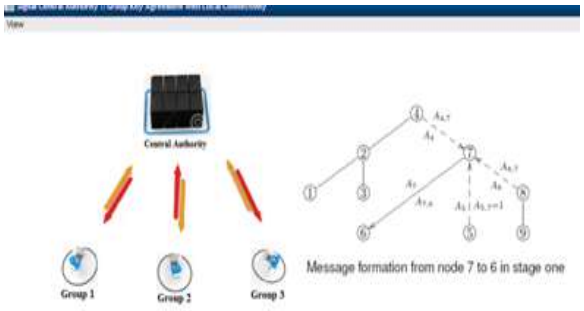

Fig 4: Central Authority

Fig 5: Registered Details

Fig 6: Group View

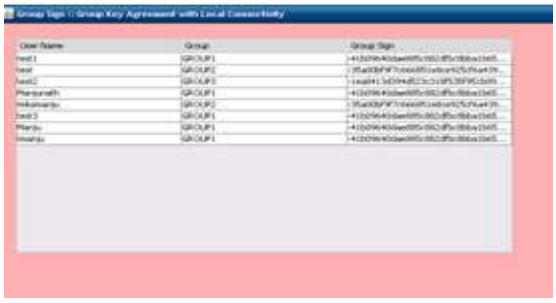

Fig 7: Group Sign with Local Users

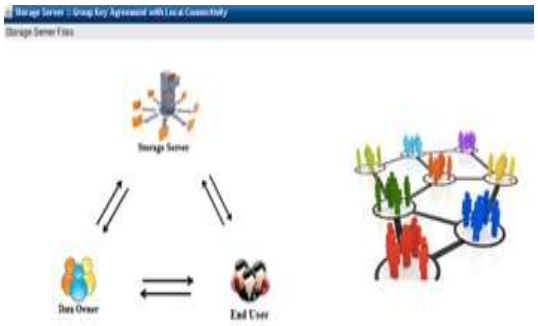

Fig 8: Storage Server Files

Fig 9: Privileges of Grouped Users

Fig 10: Attackers of Group Users

Fig 11: Group Details

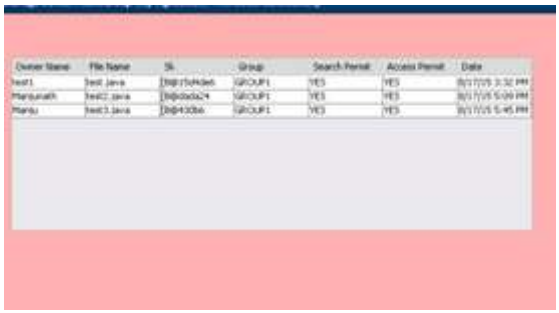

Fig 12: Storage Server Files

IV. CONCLUSION

We studied a group key agreement problem, where a user is only aware of his neighbors while the connectivity graph is arbitrary. In addition, users are initialized completely independent of each other. A group key agreement in this setting is very suitable for applications such as social networks. We constructed two passively secure protocols with contributiveness and proved lower bounds on a round complexity, demonstrating that our protocols are round efficient. Finally, we constructed an actively secure protocol from a passively secure one. In our work, we did not consider how to update the group key more efficiently than just running the protocol again, when user memberships are changing. We are not clear how to do this. One can either propose algorithms to our current protocols (as Dutta and Barua [22] did for [17]) or construct a completely new key agreement with these features. We leave it as an open question.

REFERENCES

[1] Y. Amir, Y. Kim, C. Nita-Rotaru and G. Tsudik, "On the Performance of Group Key Agreement Protocols", ACM Trans. Inf. Syst. Secur., vol. 7, no. 3, pp. 457-488, Aug. 2004.

[2] D. Augot, R. Bhaskar, V. Issarny and D. Sacchetti, "An Efficient Group Key Agreement Protocol for Ad Hoc Networks", Proc. 6th IEEE Int'l Symp. on a World of Wireless Mobile and Multimedia Networks (WOWMOM 2005), pp. 576-580, 2005.

[3] A. Beimel and B. Chor, "Communication in Key Distribution Schemes", Proc. Advances in Cryptology (CRYPTO'93), vol. 773, pp. 444-455, 1994.

[4] R. Blom, "An Optimal Class of Symmetric Key Generation Systems", Proc. Advances in Cryptology-EUROCRYPT'84, vol. 209, pp. 335-338, 1984.

[5] D. Boneh and M. K. Franklin, "An Efficient Public-key Traitor Tracing Scheme", Proc. Advances in Cryptology (CRYPTO'99), vol. 1666, pp. 338-353, 1999.

[6] D. Boneh, C. Gentry and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys", Proc. Advances in Cryptology (CRYPTO'05), vol. 3621, pp. 258-275, 2005.

[7] 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.

[8] D. Boneh and M. Naor, "Traitor Tracing with Constant Size Ciphertext", Proc. 15th ACM Conf. Computer and Comm. Security, pp. 501-510, 2008.

[9] D. Boneh and A. Silverberg, "Applications of Multilinear Forms to Cryptography", Contemporary Mathematics, Vol. 324, American Mathematical Society, pp. 71-90, 2003.

[10] C. Blundo, L. A. Mattos and D. R. Stinson, "Generalized Beimel- Chor Schemes for Broadcast Encryption and Interactive Key Distribution", Theor. Comp. Sci., vol. 200, no. 1-2, pp. 313-334, 1998.

[11] C. Blundo and A. Cresti, "Space Requirements for Broadcast Encryption", Proc. Advances in Cryptology - EUROCRYPT 1994, vol. 950, pp. 287-298, 1995.

[12] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly Secure Key Distribution for Dynamic Conferences", Inf. Comput., vol. 146, no. 1, pp. 1-23, 1998.

[13] C. Boyd and J. M. Gonz´alez-Nieto, "Round-Optimal Contributory Conference Key Agreement", Proc. Public Key Cryptography (PKC'03), vol. 2567, pp. 161-174, 2003.

[14] E. Bresson, O. Chevassut and D. Pointcheval, "Provably Authenticated Group Diffie-Hellman Key Exchange The Dynamic Case", Proc. 7th Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT'01), vol. 2248, pp. 290-309, 2001.

[15] E. Bresson, O. Chevassut and D. Pointcheval, "Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions", Proc. 21th Int'l Conf. Theory and Application of Cryptographic Techniques (Eurocrypt'02), vol. 2332, pp. 321-336, 2002.