DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5381

Volume 9, No. 1, January-February 2018

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

GROUP KEY MANAGEMENT FOR MULTICAST STRUCTURES TO IMPROVE SECURED DATA ACCESS

A. Subashini
Asst. Professor,
Department of Computer Applications
Faculty of Science and Humanities
SRM Institute of Science and Technology
Kattankulathur, Chennai

A. Jenita Mary
Asst. Professor,
Department of Computer Applications
Faculty of Science and Humanities
SRM Institute of Science and Technology
Kattankulathur, Chennai

Abstract: In the growing rapidly wireless network and mobile technology, we have one of the sophisticated techniques is multiple group key management for data security. Group key is an important function that will provide enhance better security for multiple multicast structures. An existing system performs to make the communication within a single group and it could not fix the multiple multicast group instances because of its insufficient amount of keys. The rekeying overheads are the main problem in Group key Management method. The rekeying overheads can be reduced by the Multiple Group Key Management technique. The Key Distribution Center can provide a master key and it can be generated by group keys. This will increase the data security and authorization in a better way, this will enable the access only for the authorized user to retrieve the information and restrict the access for any unauthorized users to access the information.

Keywords: Group Key Management, Master Key Encryption, Key Distribution Centre, Multiple Group Key Management, Group Controller

I. INTRODUCTION

Multicasting is one of the new and advanced techniques which is used for transferring the data from one source to many groups. Simply saying, the transmission range will get a single source received by all subnodes. Broadcasting media can be accessed by anyone and there will not be any security when the data is transmitted via air signal. The normal method is to strengthen the security control for group communication by giving the same key. It is called a group key. It should be accessed only by the member of the same group. All information may be encrypted and decrypted via this group key which will give assurance for secured communication for transferring data from one group to another group without any modification [1]. The biggest challenge will be retaining the efficient key management. Every time the members of the group should update the key information while they separating or including the group. In this juncture, the particular group will be triggered by the rekey approach. The set of GKM should be revised to solve the rekeying constraints. The multiple services were increased in the existing GKM rekeying constraints. But in a dynamic multicasting group, session key issued by group controller. In this key, the Group Controller is a secure multicast channel to allow or permit the authorized group members to access the data. The Group Controller once again provides a new session key when the group membership alteration of additions or deletions. The last and current session security will be ensured by the rekeying approach. With this approach, any new member may not be received the last sessions communications, also this will deny the access of current session to the old member who left this group. Hence, the secrecy of the group communication is managed in a better fashion.

II. MANAGING GROUP KEY BASED ON USER'S REQUEST

A Key Distribution Centre is a system that will send keys to the authenticated or authorized users in a wireless network. It will share all the confidential information along with necessary credentials. Each and every time a secure connection will be established between two systems in a wireless network. They provide request to the KDC to make a private key which will be accessed by the authorized users for validations and verifications of the data. A Key Distribution Center is in the form of symmetric encryption which will provide access of two or more multiple systems in a wireless network by regenerating a token (a type of message) to make a secure connection over that information may be shared. While communication takes place, the primary server will be connected always and accessed within the network system when establishing link any requests during the transition. It is used instead of key encoding because the private key is generated each and every time a secure connection is established, that will minimize the possibilities of hacking the information. Group key management system is a very typical functional group in multiple multicast systems. When we provide information to a set of remitters in multiple multicast services, information security can be maintained and managed in many ways. Group Controller Management needs some authentication access. Key server needs sharing of keys based on the key management architecture. Group controller management must authenticate when new members are added in a group. The members in GKM may leave any number of groups and rejoin to the old group at any time [2]. Rekeying facilities will be given for users instantly. An authorized member may convert plaintext to ciphertext and vice versa. An unauthorized user may not use the text. The

user/subscriber must have the keys to use the information [3]. Information may be in any format. Fig.1 and Fig.2 illustrate the encryption process and the architecture of the proposed work respectively.

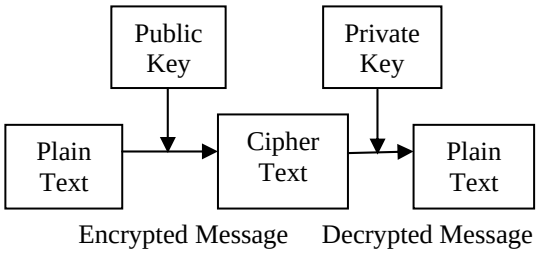

Fig. 1 Encryption Process

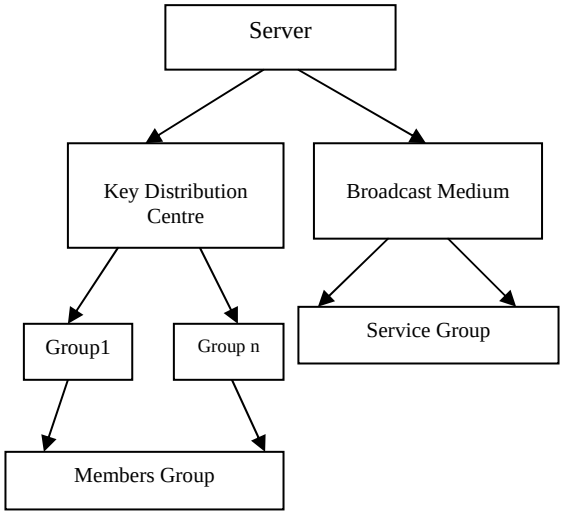

Fig. 2 Architecture of Multiple Multicast Schemes

III. PROPOSED SYSTEM

The study finds significant differences between securing uni casting communication and securing multicasting communication. The variations observed are expected to encounter scalability issues for multiple applications. As mention in the previous sections, these problems are basically varying and different in order to manage keys. Further, we prove how the differences make scalability issues for multiple applications. In this context, the Multiple Group Key Management shortly called as MGKM technique can be held the new group key management for different groups. The MGKM protocol will be retained the wireless network for single and multiple move transaction. This will result in minimizing the rekeying transmission problems.

The Master key encryption procedure will produce the master key and multiple slave keys. This technique is found very useful to provide a group key to the authorized users. It will minimize the rekeying issues by changing the asymmetry of the master and slave keys. It stated that one of the slave keys is modified; the other slave keys may remain unmodified by changing the master key [4].

The steps to make cipher text and plain text are:

- The files must be selected and uploaded to the server machine.
- Make the cluster formation of subscribers and for each subscriber inside the cluster, a separate IP address is formed. For each and every cluster a slave key is dynamically formed using random methods.
- The output file will be in ciphertext format.
- Area key and domain key are important keys to decrypt the file.

This system contains two modules: Registration module, Key Generation Module.

A. *Registration form for authorized members*

Each and every authorized member should key in the required data and register through server machine. Then server machine will provide authorization for accessing multiple services. Each member has to give group name, subscriber id and subscriber name to form a group. Fig. 3 shows the User Interface Screen for registration.

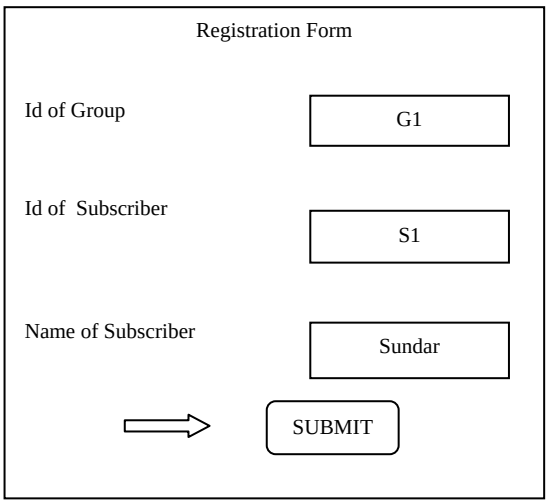

Fig. 3 Group Formation

B. Key Generation Module

Group key management is concerned with making and modifying secret keys. It is the fundamental technique to make secure multiple multicast communications. Key Management facilitates the information secretly and access controls by confirming that the keys are used to encrypt multiple multicast communications to share only authorized users. The group key distribution centre has the two most important security methods called as forward and backward secrecy, which produces the group management key [5].

IV. CONCLUSION

This technique has the advanced security system on the data communication and it will encourage only the authorized users to access the information through the group key management system. The proposed methodology ensures minimization of rekeying process and it is found very simple when compared to other systems. The advantage over the existing methods is the less utilization of memory to store the keys. Also, it is observed that the procedure is less complex.

V. REFERENCES

[1] T.T. Mapoka, "Group key management protocols for secure mobile multicast communication: A comprehensive survey", Int. J. Comput Appl., vol.84, 2013, pp.28-38.

[2] D.M.Wallner, E.J.Harder and R.C. Agee, "Key Management for Multicast Issues and Architectures", http://www.ietf.org/rfc/rfc2627.txt, 1999.

[3] C.K. Wong, M.G. Gouda, and S. Lam, "Secure group communications using key graphs", ACM SIGCOMM Computer Comm. Rev., Vol. 28, 1998, pp.68-79.

[4] Qiong Zhang**,** Yuke Wang and Jason P. Jue, "A Key Management Scheme for Hierarchical Access Control in Group Communication", International Journal of Network Security, Vol. 7, No. 3, 2008, pp.323-334.

[5] Y.Challal and H.Seba, "Group Key Management Protocols: A Novel Taxonomy," International Journal of Information Technology, Vol. 2, No. 1, 2005, pp. 105-118.