AN EFFICIENT AND SECURE GROUP KEY MANAGEMENT SCHEME IN MULTICAST NETWORK USING CLIKEv2

[1]S.Thilagam, [2]Dr.N.M.Saravana Kumar

[1]PG Scholar,Dept. of IT,Vivekanandha college of Engineering for Women, Tiruchengode, India.
[2]Prof. & Head, Dept. of IT, Vivekanandha college of Engineering for Women, Tiruchengode, India.
[1]thilak1993it@gmail.com, [2]saravanakumaar2008@gmail.com

Abstract: Group key management plays a vital role in group communication. Secure group communication can be achieved by the use of group key. Several group key management schemes have been proposed. This paper proposes an efficient and secure group key management scheme in a multicast network for achieving a secure communication between members of a group as well as ensuring better forward and backward secrecies. In this scheme, the static group key is generated to makes the group communication in an efficient way. It aims at providing better security with the help of Certificate-less Internet Key Exchange version2 protocol. It eliminates the use of certificates, cookies during an authentication process. It uses Elliptic Curve Diffie-Hellman Key Exchange instead of RSA based Diffie-Hellman Key Exchange. It affords the same security level as RSA with reduced key size. The computation and communication overhead of the proposed scheme is to be reduced with these techniques. Furthermore, the proposed scheme is compared to some existing key management schemes.

Keywords: Group communication, key management, Certificate-less Internet Key Exchange v2 (CLIKEv2), Group key generation, subgroup key generation, Authentication, Rekeying.

1. INTRODUCTION

1.1Group Communication

Group communication refers to the interaction between members of a small group of individuals. In the modern internet world, the multicast network is popular for group communication. But the main impasse of a multicast network is security.To provide the security we are using many keys like public key, private key, Group key, Session key, etc.. A primary method for limiting access to information is through encryption and selective distribution of keys used to encrypt group information. The keys used for this purpose are cryptographic keys.

In group communication, the group key is generated and it is distributed to all members of the group. Only by using this key each member can communicate with other members in a group. Before starting communication, a message is encrypted with a group key. An authorized person can decrypt the message by using a group key which was previously distributed.

Member can join or leave a group at any time. Whenever a new member joins a group they shouldn't encrypt or decrypt the messages which were previously exchanged in that group. This implies backward secrecy. Similarly, whenever an existing member leaves a group they shouldn't encrypt or decrypt the further messages. This implies forward secrecy.

1.2 Key Management

Managing cryptographic keys is a major role in group communication. To maintain forward secrecy and backward secrecy, the keys must be regenerated for every modification in the group. This process is known as Rekeying.

The number of messages needed to update keys must be less. There are a number of architectures exist for group communication like minimal key storage, Logical key hierarchy, Hybrid architecture, etc... In these existing architectures, key generation depends on members of a group. Also, a number of messages required to updatekeys are high, keys like group key, cluster key are needed to be regenerated during membership changes to maintain dynamism and secrecy of a group. Due to this, the existing schemes consume more computation and communication overhead. Hence, the main goal is to reduce communication and computation overhead.

1.3Certificate-less Internet Key Exchange version 2

Internet Key Exchange is a secure key exchange protocol and used for policy negotiation and to set up

a security association (SA) in the IPsec protocol suite. It is used for mutual authentication and establishing a shared secret session key to create an IPsec SA. A security association is the establishment of shared security attributes between two network entities to support secure communication. It includes attributes such as cryptographic algorithm and mode, traffic encryption key and parameters for the network data to be passed over the connection. In advance of an IP packet being protected by IPSec, IKE creates SAs dynamically in support of IPSec and manages the Security Association Database (SAD).An Earlier version ofIKE uses X.509 certificates for authentication either pre-shared or distributed using DNS and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

IKE has two versions namely IKEv1 and IKEv2 respectively. IKEv1 is based on IPSec SA whereas version 2 is based on child SA. The protocol is a request-response type with a sender and a receiver. IKE consists of two phases:

Phase I: It ensures mutual authentication and establishes session keys. It is based on identities and secrets as public key parameter or pre-shared secrets between the two peers. It also establishes an IKE SA.

Phase II: By using IKE SA which is established in phase I, multiple phase II SAs between the same peers of entities can be established which is called IPSec SAs.

There are two exchange modes in version1 namely main mode and aggressive mode. It accomplishes the task in 3 messages and 6 messages respectively. The former mode is faster and the latter one is more flexible. IKEv1 use four types of authentication methods such as Pre-shared Key(PSK), Digital Signature(RSA-Sig), Public Key Encryption, Revised Mode of Public Key Encryption. Whereas in IKEv2 Pre-shared (PSK), Digital Signature (RSA-sig) only used. In IKEv1, both peers must use the same authentication method whereas IKEv2 can use different authentication method in various peer.

IKEv1 is certificate based whereas version 2 is certificate less based key exchange. It eliminates cookies, public key certificates. It provides a mutual authentication.

In existing schemes, authentication process consumes more time and needs additional keys. To overcome these complications, the proposed scheme uses the phase-I process of CLIKEv2. It eliminates the needs of additional keys. Moreover, it prevents communication from the attacks such as replay attack, Man-in-the-middle attack, Non-repudiation.

The remaining part of this paper organized as follows: section II deliberates some of the related works, section III explains the detailed explanation of the proposed scheme, section IV gives the analysis report on the proposed scheme and section V concludes the paper.

2. RELATED WORKS

Several key management schemes for the multicast networks such as Logical Key Hierarchy (LKH), Hybrid Tree Distributions etc. are listed and explained in [2]. Also, they propose a new key management in dynamic multicast networks that decreases the structure to cluster based for providing security.

One of the commonly used key management scheme is a logical key hierarchy which is explained in [3] reduces key storage. But, it needs to regenerate a number of keys during membership changes to maintain forward and backward secrecy.

A cluster based enhanced key management scheme is described in [4] reduces the computation and communication but it consumes more key storage space.

An Efficient Distributed Group Key Management Using Hierarchical Approach is designed in [5] for many-to-many communication. It is based on ECC which decreases the key length and using logical key hierarchy architecture. This scheme takes zero rekeying operation for joining and one rekeying operation for leaving.

Scalable and Reliable Cost Effective Key Agreement Protocol for Secure Group Communication [6] reduces the number of messages needed during the time ofrekeying and the number of keys stored in servers as well as members and hence the cost of computational overhead is reduced.

Certificate-less Key agreement protocol for IKEv2 used in Internet of Things is described in[7]. It is based on certificate less key agreement protocol. It eliminates cookies, certificates during authentication process by using IP address and ID.ECCDHKey Exchange is used inIKEv2.

It takes minimum storage capacity and minimum computation cost.

ECC-Based IKE Protocol Design for Internet Applications[8] explains how the Internet key exchange is obtained by using Elliptic curve cryptography Diffie-Hellman Key Exchange. This scheme avoids cookies, public key certificate during the authentication process.

A survey on group key management schemes which is presented in [9] describes various approaches to group key management and its challenges in network dependent and network independent approaches.

A Proactive Secret Sharing is explained in [10] to cope with perceptual leakages. It splits the secret into n shares and these shares are distributed to n members. In the receiver side, k shares among n are combined and get the secret.

Various clustering schemes for efficient group communication is discussed in[11]. Also, it discusses the comparison between various clustering schemes in terms of computation cost and communication cost. Moreover, it describes the cluster head selection algorithm.

3. PROPOSED SCHEME

The proposed scheme is based on time-based cluster structure. In this structure, subgroups are formed based on the timestamp. The scheme has three entities such as Group controller (GC), Subgroup Controller (SGC) and Group Members. GC controls entire group and defines a number of subgroups in it. Based on the member's subscription span value, they are assigned to a relevant subgroup by GC.Each subgroup is handled by individual subgroup controller (SGC). SGC controls only the members under it. Each member of the group has unique ID (UID) and public-private key pair. GC maintains two databases namely present member database(PMDB) and Leaving member database (LMDB). The former contains the details of all members currently present in a group and the latter contains the details of leaving member. To attain secure communication, group key(GK) and subgroup key(SGK) is generated. The GK is static which is generated only once because it is independent of the group members, depends only on SGCs. If there are any membership changes in a network, subgroup key of the relevant modified subgroup will be regenerated.There is no need to regenerate group key. To establish communication, eachmember must be authenticated with each other throughcertificate less Internet Key Exchange version2 protocol.The architecture of this cluster structure is shown in Fig.1.

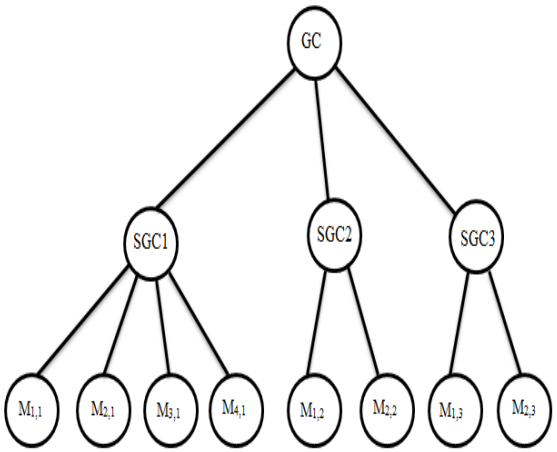

Figure 1: Architecture of cluster structure

This scheme consists of following steps/modules:

1. UID generation
2. Group Key and Subgroup key generation
3. Generation of Public-Private keys
4. Communication and authentication
5. Rekeying

3.1 UID Generation

After assigning a member to the subgroup, SGC generates UID. To generate UID, GC sends a randomly generated binary value to each SGC and SGC generates a random binary value to each member under it. The final UID is obtained by appending uniquely generated binary values from SGC to commonly received binary values from GC. Then, it is distributed to GC and respective member. At the end of this step member details with their UID is stored into the PMDB.

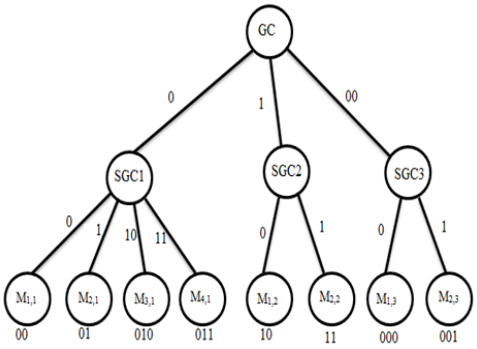

Figure 2: Huffman coding generation

3.2 Group key and Subgroup Key generation

Subgroup key generation:

Subgroup key is generated by SubgroupController. It is used for intra-subgroup communication. For SGK generation,all membersof that subgroup send its partial key to their corresponding SGC.After receiving partial keys, SGC XORs these with its own partial key. The partial key is a random prime number. Each member's partial key is denoted as $f^{L_{i,j}}$ where i=1,2,3,.. and j=1,2,3,… Here f is the generator of the multiplicative group,Z_N^* which is the set 1,2,..N-1 where N is the prime and L is randomly chosen prime number of the respective member. For example, the partial key of member 1 of SG1 in fig.1 is $f^{L_{1,1}}$.

The partial key of SGC is denoted as f^{k_i}. For example, in the fig.1 partial key of SGC1 is f^{k_1}. Therefore, final subgroup key of SGC1 is obtained by using following equation,

$$SGK_1 = f^{k_{1,1} \oplus k_{2,1} \oplus k_{3,1} \oplus k_{4,1} \oplus k_1}$$

This Subgroup key is sent to all the members under it for further communication.

3.3 Group key generation:

Group key is generated by GroupController. For GK generation, each SGC sends its partial key to group Controller. GC XORed these partial keys with its own partial key. The partial key of GC isf^k. Therefore, final group key for fig.1 is obtained by using following equation,

$$GK = f^{k_1 \oplus k_2 \oplus k_3 \oplus k}$$

This group key is sent to all the members and Subgroup controller under it for furthercommunication.

The SGKs and GK are distributed by using proactive secret sharing scheme. For each GK and SGK distributed to the sub-groups and the members, time periods, T_{GK}andT_{sGK}, are set and divided into periods of time. Here, a proactive threshold scheme is applied, say (r + 1, t), where, t is the number of time periods and r + 1 is the number of locations, say routers on the way between the sender and receivers, to be compromised by the adversary, who tries to learn the GK or SGK, in a single time period which is difficult as at the end of each time period, the share becomes obsolete and has to be erased. It is even difficult to distrust the secret by the adversary as t − r shares are to be corrupted in a single period of time.

3.4 Public-Private key Generation

- Each member in a group has a public-private key pair. These keys are used during authentication process. This public-private key pair is generated based on ECC algorithm. Private Key, d where, d is a random prime number.
- Public Key, PU = PR*B

  where, B is a base point in an elliptic curveand is a public parameter.

  * is a scalar multiplication.

3.5Authentication and Communication

Before starting communication, all members must be authenticated with each other. Authentication is done by using certificate less key agreement protocol. The proposed scheme is based on CLIKEv2. It eliminates the use of certificates and cookies from the traditional protocol. It is ECC based and parameters of the elliptic curves are agreed upon by both communicating entities. The sender must know the receiver's UID and IP address and vice versa to initiate key negotiation. The IP address of the receiver is unique and his system is password protected.

As described in section I, CLIKEv2 established in two phases. Among these, a phase-1 operation is used in the proposed system for establishing mutual authentication between group members and session key generation.

Phase-1:

The steps involved in phase-1 are described as follows:

Step 1: Sender →Receiver: HDR, SA_i

The sender sends the HDR and security association that contains cryptographic solutions to the receiver.

Step 2: Receiver → Sender: $HDR, SA_i, PU_r, Flg_r, N_r$

The receiver calculates a digest, $Flg_r = h(IP_r, UID_r, PU_r)$ and selects the required cryptographic algorithms from the offered solutions. Then receiver sends these values along with its public key and nonce. The nonce is a unique random number and is used only once during authentication. This value should not repeat in another communication. It prevents the replay attack. If the receiver is not satisfied with the offered cryptographic solutions it will send an error message in this step.

Step3: Sender→Receiver:

$HDR, PU_i, Flg_i, E_{k_x}(N_r || N_i || IP_i)$

The sender computes its own $Flg_r$and compares it with the received value. If it is not match the communication is terminated. Otherwise, the initiator calculates the session key from the received public key of receiver.

$$SK = d_i * PU_r = (k_x, k_y)$$

Now, sender generates its own Flg_i and transmits it with its public key, encrypted nonce of sender, receiver and its IP. Hence, the receiver is verified and replay is checked.

Step 4: Receiver → Sender: $E_{k_x}(N_r || N_i || IP_r)$

The receiver verifies the digest of sender Flg_i, if it matches with received value then calculates the session key using public key of receiver. Now, it sends the encrypted values of the nonce of sender and receiver along with its IP to sender for mutual authentication.

If the session keys which are generated in sender side as well as receiver side are same, then the members are mutually authenticated. Once the authentication is attained, the sender and receiver can exchange message. Furthermore, they are agreed to calculate derived keys like authentication key, encryption key from the session key elements.

3.6 Rekeying

The main motivation of group communication is to maintain the dynamism of group which means any member can join or leaves a group at any time. Whenever a membership changes occur in a network, rekeying should be done. There are two operations namely leaving operation and joining operation that will occur during existing members leaves from a group and new member joins a group respectively.

3.6.1 Leaving Operation

Whenever a member wants to leave a group, it sends a request to GC. GC removes the data about that member from PMDB and stores it in a LMDB. After removing process, a subgroup key of that particular subgroup needto be regenerated as described in the section 3.

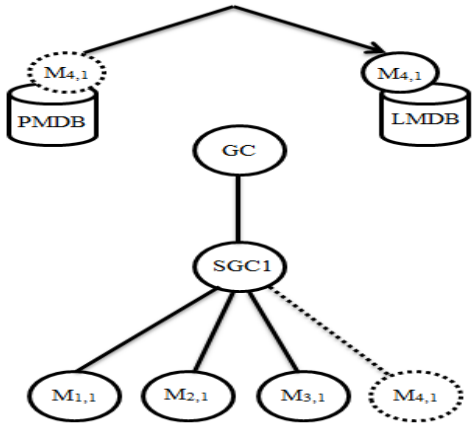

Figure 3: Leaving operation

In Fig.3 member 4 ($M_{4,1}$) under SGC1 wants to leave from a group. $M_{4,1}$sends a leave request to GC. GC removes the data about that member from PMDB and insertsit into the LMDB. After leaving, SGC1 regenerates SGK1 and distributes it to all remaining members under it. GK remains same. If $M_{4,1}$ wants to communicate with the group member, he/she can't able to communicate because of the modified SGK1. Therefore, $M_{4,1}$ cannot read the further messages that are exchanged in the group. Hence, it maintains forward secrecy.

3.6.2 Joining Operation

Whenever a new member wants to join a group, it sends a request to a GC. The GC assigns it to a respective subgroup based on a subscription span value. After that, UID will be generated and sends it to the relevant member. Then GC sends its GK to that new member. SGC changes its own key value (SGK) and sends it to the entire member under it.A member generates a public-private key pair of its own. These keys are generated as described in section 3. Then GC inserts the details about that member in a PMDB. Now, a new member can communicate with any of the membersin that group. But this new member can't read the messages which were previously shared between the members.

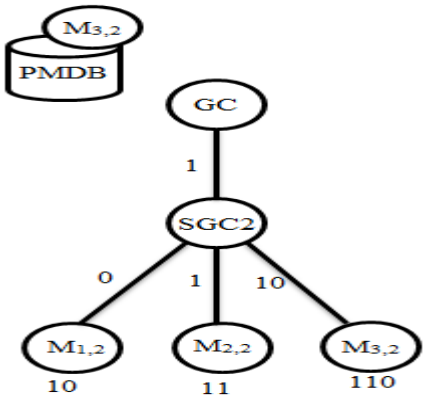

Figure 4: Joining operation

In Fig.4 a new member $M_{3,2}$ wants to join a group. At first, it sends a join request to GC. The GC accepts a join request and allocated it to a subgroup 2 (SGC2). After that UID is generated and SGC2 regenerate its own key as described in section 3. Now, a new member can communicate with any of the members in that group. Hence, it maintains the backward secrecy.

The overall framework of the proposed scheme is shown in Figure 5.

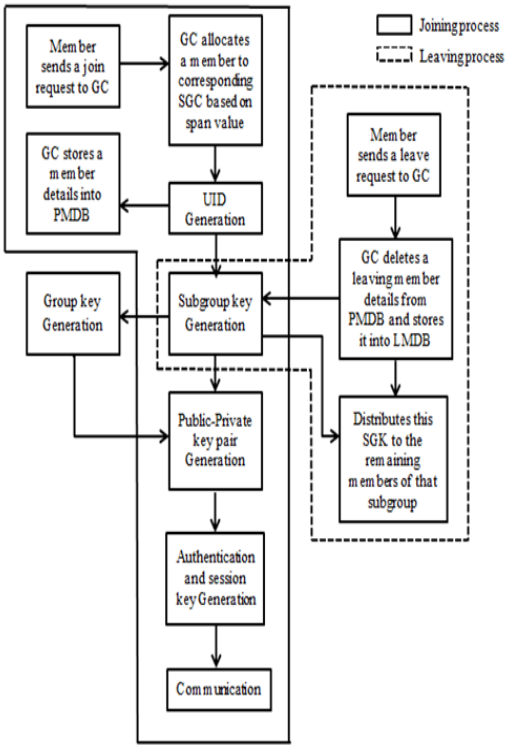

Figure 5: Framework of the proposed scheme

4. ANALYSIS

The performance of the proposed system is compared to some of the existing systemssuch as Logical key Hierarchy and One way function tree in terms of communication and computation cost.

4.1Communication Cost

Whenever a membership changes occur, databases maintained by GC will notify it to the SGC. Now, the SGC can identify the changes in a group. Therefore, only one message is sufficient for informing the modification. Hence, the communication cost of the proposed system is O(1). Table 1 shows that the comparison between existing and proposed scheme in terms of communication cost.

Table 1: COMMUNICATION COST

	Join	Leave
OFT	$\log_2 n + 1$	$\log_2 n + 1$
LKH	$2\log_2 n - 1$	$\log_2 n$
Proposed Scheme	1	1

4.2Computation cost

Whenever a SGC receives the information about modification in group members, it regenerates its key to maintain forward and backward secrecy. There is no need to change the group key because it is independent of the group members. Therefore, we have to modify only one key. Hence, the computation cost of the proposed scheme is O (1). Moreover, the authentication process in the existing system requires two more public keys for each member. These two are only used for an authentication process. But the proposed authentication scheme avoids the need of using additional keys. Hence, it reduces the computation cost and a number of keys stored by each group member. Table 2 shows that the computation cost of the existing and proposed scheme.

Table II. COMPUTATION COST

	Join	Leave
OFT	$\log_2 n + 1$	$\log_2 n + 1$
LKH	$2\log_2 n - 1$	$2\log_2 n$
Proposed Scheme	1	1

5. CONCLUSION

The aforementioned key management scheme for multicast network provides higher level security. It is an efficient method for maintaining forward and backward secrecy during membership changes in a network. The certificate-less Internet Key exchange version2 offers mutual authentication with a minimum number of messages exchanges. ECC algorithm for key generation and key exchange provides the same security level as RSA with reduced key size. Static group key reduced the computation cost. The analysis report explains that the proposed scheme reduced communication and computation overhead when compared to some of the other existing key management schemes. From these, we can conclude that the proposed scheme is secure and efficient for key management in group communication.

REFERENCES

[1] N.M.Saravana Kumar, T.Purusothaman, "SEGKMS: Scalable and Efficient Group Key Management Scheme in Multicast Networks" European Journal of Scientific Research ISSN 1450-216X Vol. 89 No 3 October, 2012, pp.394-408.

[2] R. Srinivasan, V. Vaidehi, R. Rajaraman, S. Kanagaraj, 2010. "Secure Group Key Management Scheme for Multicast Networks. International Journal of Network Security", Vol.11, No.1, PP.33{38).

[3] Wu tao, Zhengxue-feng, Bai li-zhen, (2009), 'A new scalable key-management scheme for secure multicast', DOI: 978-1-4244-9763-8/11.

[4] Saravana Kumar Muthusamy, PurusothamanThiyagarajan and LavanyaSelvaraj, "An enhanced and cost effective group key management scheme for multicast network". Journal of Computer Science, 9 (4): 477-487, 2013,ISSN 1549-3636,© 2013 Science Publications; doi:10.3844/jcssp.2013.477.487 Published, Online 9 (4) 2013.

[5] Shikha Sharma, C. Rama Krishna, "An Efficient Distributed Group Key Management Using Hierarchical Approach with Elliptic Curve Cryptography" 2015 IEEE International Conference on Computational Intelligence & Communication Technology, DOI 10.1109/CICT.2015.116

[6] S. Jabeen Begum and Dr.T. Purusothaman, 2011. "A New Scalable and Reliable Cost Effective Key Agreement Protocol for Secure Group Communication" Journal of Computer Science 7 (3): 328-340.

[7] M.Lavanya, V.Natarajan, "Certificate-less Key agreement protocol for IKEv2 used in Internet of Things".

[8] Sangram Ray, RachanaNandan, G. P. Biswas, "ECC Based IKE Protocol Design for Internet Applications", Published by Elsevier Ltd. doi: 10.1016/j.protcy.2012.05.083

[9] R. Seetha, R. Saravanan, "A Survey on Group Key Management Schemes", Cybernetics And Information Technologies, Volume 15, No 3, ISSN: 1314-4081, DOI: 10.1515/cait-2015-0038.

[10] A.Herzberg, S.Jarecki, H.Krawczyk, M.Yung, "Proactive Secret Sharing or How to Cope with Perpetual Leakage". CRYPTO'95 Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology, pp-339-352, Springer-Verlag.

[11] S. Jabeen Begum and T. Purusothaman, "Hierarchical Tree Structure Based Clustering Schemes for Secure Group Communication" , Springer Science+Business Media New York 2015.

[12] Keerthana R., Dr.SaravanaKumar N.M. (2014), 'A Cost Effective Multicast Key Management Scheme for Secure Group Communication', International Journal of Innovative Research in Computer and Communication Engineering, ISSN:2320-9801, Vol.2, Special Issue 1, pp:1177-1183.

[13] Mythili G.M., SaravanaKumarN.M. (2014), 'Dynamic Architecture for Scalable and Proficient Group Key Management', International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320-9801, Vol.2, Special Issue1, pp:1177-1183.

[14] SonaliPatil, Nikita Rana, Dhara Patel, Prajol Hodge(2013), 'Extended Proactive Secret Sharing using Matrix Projection Method', International Journal of Scientific & Engineering Research, ISSN 2229-5518, Vol.4, Issue 6,pp:2024-2029.

[15] Saravana Kumar N.M., Ramachandran S., Lavanya S., (2013), 'A Cluster based Cost Effective Group Key Management Protocol for Multicast Network',International Journal of Computer Applications, pp: 22-30.

[16] 'Diffie-Hellman Key Exchange', www.math.brown.edu/~jhs/ MathCrypto/SampleSections.pdf.