Mobile Networks and Applications (2019) 24:1152–1159
https://doi.org/10.1007/s11036-019-01252-4

Secured Key Management Scheme for Multicast Network Using Graphical Password

S. Lavanya[1] · N. M. SaravanaKumar[2] · V. Vijayakumar[3] · S. Thilagam[2]

Published online: 1 May 2019

Abstract
In recent days, management of keys in a group has become a significant part of data communication. The textual and alphanumerical passwords used for security concern have now changed its trend to different graphical passwords procedures. Many researchers have introduced various efficient and scalable key management schemes and it is difficult to remember this type of password. There are many textual password authentication mechanisms now available in the software market and are prone to eavesdropping, dictionary attacks and shoulder surfing. To address all the above vulnerability, many researchers and practitioners have developed different authentication methods who are interested in finding an alternate way to the existing problem. Hence, this paper proposes a secure group communication scheme between group members using graphical passwords and this is easy to remember compared to a textual password but difficult to hack. The elliptic curve cryptography technique is applied for key distribution. The group key is a graphical password which is static and shared among all the members in a group. The sequence of images will be sent to the members/users of a group during registration to form a group key and the group controller sends a pass point value of each image to the member by using elliptic curve cryptography after the registration. The main focus of the proposed scheme is to provide better security and ensures negligible communication overhead and computation overhead.

Keywords Group communication · Graphical password · Rekey · Elliptic curve cryptography (ECC)

1 Introduction

1.1 Group communication

Group communication refers to the process of communication among members of a small / large group of individuals. In the modern internet world, multicast networks have gained popularity for group communication. But the core dilemma of multicast network is its security. The group information should not be accessed by non-group members. A primary method for restrictive access to facts is through encryption and discriminatory distribution of keys used for encrypting group data and the key used for this purpose is known as cryptographic key.

Two types of keys specifically symmetric and asymmetric key are available in cryptography. The symmetric key could be applied for communication in group, which is named as group key [1]. It is used for encryption and decryption process to offer secure communication. To send or receive group information or message to a particular group, every authenticated member should know the group key of that particular group. Each member has his/her own public and private key for one to one communication between the members within a group. The communication is organized using either public or private asymmetric key. In addition to these keys, session key is applied for validation purpose. A secure group communication is attained using all these keys.

As and when new member requests to join in a new group or previous users wants to remove from the group, a new authentic key gets regenerated for that particular group to

✉ S. Lavanya
lavanyamecsbit@gmail.com

N. M. SaravanaKumar
saravanakumaar2008@gmail.com

V. Vijayakumar
vijayakumar.v@vit.ac.in

S. Thilagam
thilak1993it@gmail.com

[1] Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India

[2] Vivekanandha College of Engineering for Women, Tiruchengode, Tamilnadu, India

[3] VIT University, Chennai, Tamilnadu, India

achieve secure communication. Handling those keys is a major role in group communication which is known as key management.

1.2 Graphical password

Graphical password is a picture or a pattern - a type of password used for the purpose of authentication. In this type, the users click on the images or draws correct patterns to authenticate themselves. It is an alternative approach to an alphanumeric password.

Recall and recognition based methods are the two main processes of graphical password. It includes many techniques namely DAS (Draw a secret) scheme, signature scheme, PP (Pass Point) scheme which are the ones classified under the Recall Method. Dhamija, Perrig scheme and the passface scheme that deals with two factor authentication ensures strong security [2, 3] based on Recognition-based technique.

Generally cryptographic keys are textual password which may be characters, numbers and alphanumeric. To provide a strong security, setting up a complex password is highly required with characters, special characters, and numbers, etc. and these types of complex passwords are difficult to remember. To overcome this problem, group key is generated based on graphical password scheme and is disseminated to all the users of a group. The issues present in key management schemes are the passwords that could easily get cracked by non-trusted parties via communication. To add to this the computation cost is usually very high.

The proposed scheme is a cluster-based structure in which the group key, subgroup key, public and private keys are used for secure group communication. The graphical password is formed based on pass point and signaled click point technique which are used for key generation and authentication process.

Group controller generates a graphical password which acts as a group key and is dispersed to all the users/members of the group. The Subgroup key is also generated in the same manner and is distributed to every member of that subgroup. Each member can communicate with others only by using these key values. Before the data communication is established, all the messages should be encrypted and sent to the corresponding members within a group. An authorized user can get into the valid graphical password which is already distributed to the group and the subgroup controller. The encrypted message received by the member is decrypted using the graphical key. If an unauthorized person or non-group member receives a message then they would not be able to decrypt it. Hence, the communication is said to be secure and established.

When a new user or a member joins the group he/she cannot encode or decode the existing messages present in the group. This suggests the backward secrecy is ensured. Similarly, when a present member exits the group future encryption or decryption of messages in that group would be prevented. This implies that the forward secrecy is ensured. The keys in a group should be changed for every modification (Leave/Join) to guarantee forward and backward secrecy. The key modification is based on the graphical password method. Hence, it provides secure communication.

The main objective is to provide strong security for data communication over a network. The security can be provided through graphical password strategy. When dealing with graphical formats, it is highly important to take care of communication and computation cost which is supposed to be justifiable. So, this research aims in providing strong security with negligible communication and computation cost. Of course justifiable cost needs to be accepted when the provision of security is strong enough.

1.3 Paper organization

The residual part of the research work could be structured as follows, Section 2 elaborates on the various existing methods of key management and graphical password. Section 3 explains the proposed scheme. Section 4 gives the detail comparison between the proposed and previous schemes. Section 5 gives the conclusion and future scope of the proposed work.

2 Related works

A number of key management patterns for the multicast networks are described in [4]. The authors also proposed a novel key management in dynamic multicast networks that organizes the network into clusters for providing security. The group controller sends the public key of the authentic members to the subgroup controller.

A secure method for cost optimization is designed for a one sender and multiple receivers which are explained in [5] is a novel technique for improving communication restrictions. The proposed method is based on a hybrid tree so that the storage and update communication depend on the tasks related to the cluster size.

In [6], the group communication was secured using keys based on elliptic curve cryptosystem. The proposed method offers security using a small key size. This method is well-organized and best suited for cluster based communication network. It supports single join and single leave operations/events. The rekeying procedures are assumed in a manner which is quite periodic.

A hierarchical and efficient distributed group key management [7] is designed for many-to-many communication and is based on an elliptic curve cryptography, which has a decreased key length and logical key hierarchy structural design.

This scheme takes zero rekeying operations to join and one rekeying operation to exit the group.

Design of Secure Group Key Management method for Multicast Networks by Number Theory was given in [8]. The proposed method secures the dynamic multicast networks adeptly. The benefits of LKH and Chinese Remainder Theorem are taken into consideration to ensure key management effectively and it further summarizes few other key management schemes.

An agreement Protocol for scalable, reliable and secure Group Communication [9] is designed for reducing computational and communication overhead as well as its ability to generate smaller size group key with the notion to attain high level security.

A review on multicast key management scheme is described in [10]. It examines problems in multicasting domain and discusses some distinctive patterns which resemble the Simple Key Distribution Center (SKDC) and it gives the comparison between various key management protocols for secrecy, storage, number of keys needed to be changed during joining and leaving procedures [11].

Petrick's method [12] is implemented for dealing with various methods when a user leaves the group.

Novel approach presented in [13] are Huffman and Petrick based methodology. Petricks method is employed when multiple users exit from the group. The method aims to lessen the great overhead in distributing the keys [14].

A Proactive Secret Sharing or a Perpetual Leakage is explained in [15] splits the secret into n shares and these shares are distributed into n members. In the receiver side, k shares among n are combined to get the secret message. Also it explains how to cope with leakage.

A User Authentication by Secured Graphical Password is explained in [16]. It explains the comparison between textual password and graphical password. Also it explains various graphical password techniques like set of regions, set of points, draw a secret and comparison of these various techniques. It proposes a new scheme by combining the pass point and random questions.

3 The proposed scheme

The real time scenario identified to proceed with this research is Pay channel. Consider a service provider who is providing their services as different channels to the users. The sample channels include Discovery(C1), NDTV(C2), National Sports(C3), etc. The service provider would like to provide services by transferring channel data to the subscribed users alone in a secured manner. The above setting has been transformed in to a clustered architecture or a structure which consists of three levels said to be hierarchical order such as GC level, SGC level, GM level. All group members are sub grouped based on their own subscription span value(1 year subscription for channel C1, 6 Months subscription for channel C2, 3 months for channel C3 and so on which refers to the life time of the particular member in a group. Initially, Group controller (GC) assigns a number of subgroups under it statically. Each subgroup is handled by individual subgroup controller (SGC) that has the overall control over group members. The architecture of this cluster structure is shown in Fig. 1. In this figure, there is one group controller (Considering only one channel), three Subgroup Controllers namely SGC1, SGC2 and SGC3 which controls 3, 2 and 2 members respectively. The member of the group is named in such a way that M is a j_{th} member present in the i_{th} group named as M_{ij} where i = 1,2,….n and j=,2,……x, both n and x is an integer value. The GC is a service provider, SGC is a service distributer who takes care of subscription and data provision based on the subscription, value/time and the users who are making use of the network..

The overall process of the proposed technique is described in this section. The workflow of this technique is shown in Fig. 2. The steps are:

1. UID generation
2. Group Key and Subgroup key generation
3. Generation of Public-Private keys for individual member
4. Communication and Authentication

Initially a user/member who is interested in joining a group transmits a request along with its subscription span value to group controller. GC assigns a member to a particular SGC wherein SGC generates a Unique ID for the newly joined member.

For secure communication [17] we need to generate group key and subgroup key based on graphical password which is described in section 3.2. For unicast communication, the public and the private key of the member are generated. After

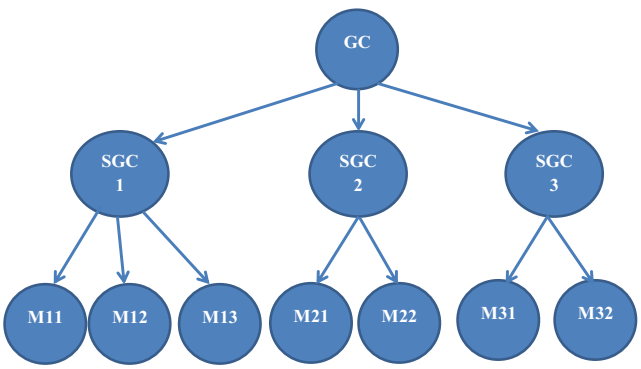

Fig. 1 Architecture of cluster structure

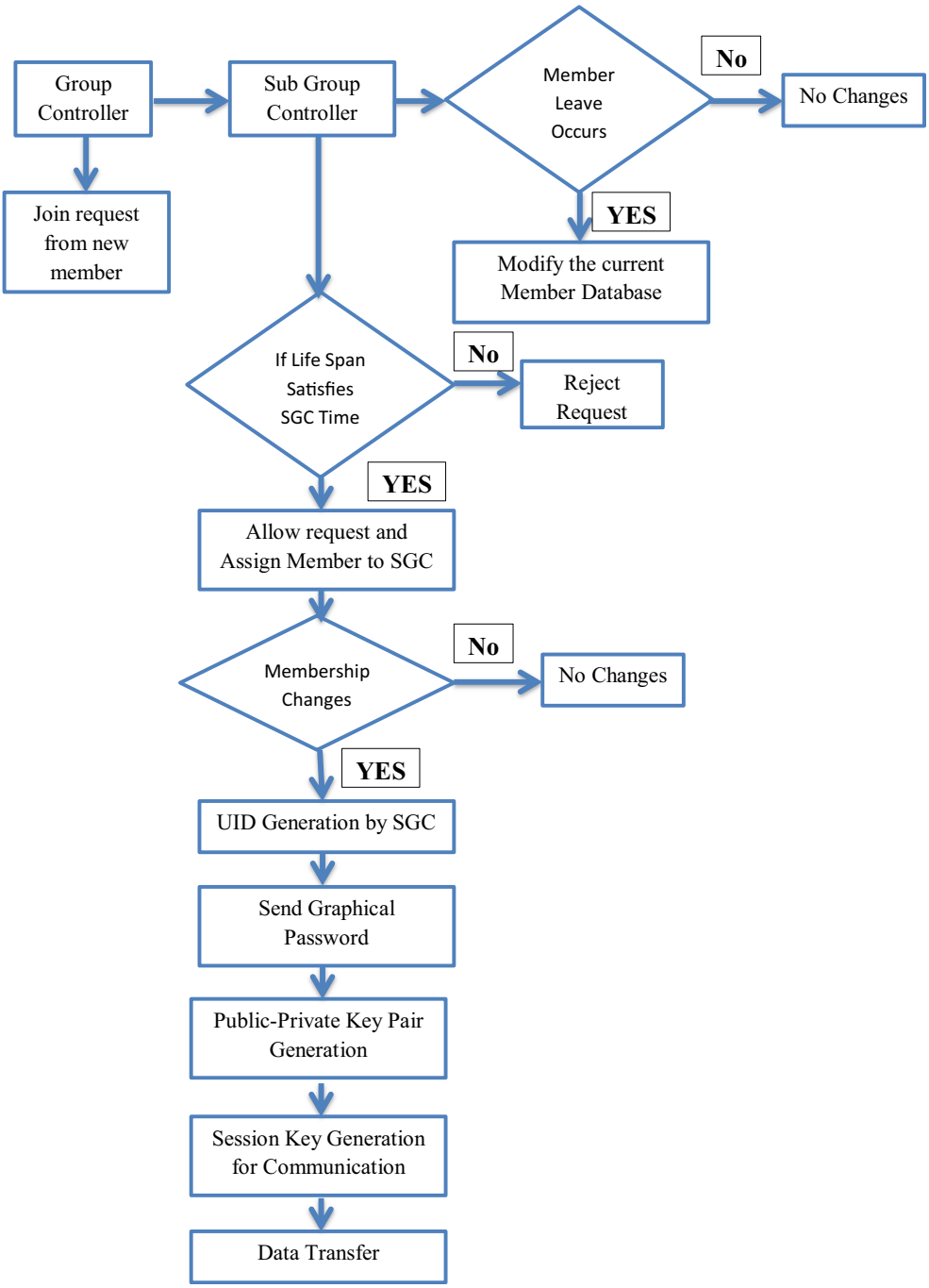

Fig. 2 Workflow of the proposed scheme

generating all these key values, communication takes place as described in section 3.4. If there is any change in a group then rekeying has to be done for ensuring forward and backward secrecy.

3.1 UID generation

UID is a unique identity and each member in a group has their own UID, which consists of a combination of binary values received from Group Controller and the binary value from SGC which are unique. GC assigns unique binary values to each SGC. SGCs generate binary value using modified Huffman coding technique. The final UID is attained combining the above said two binary values. This is shown in Fig. 3.

3.2 Group key and subgroup key generation

Group Key (GK) is generated by using a graphical password instead of textual password by a group controller. This group key generation [18] is independent of the subgroup controller. There are set of images stored by GC and these images are

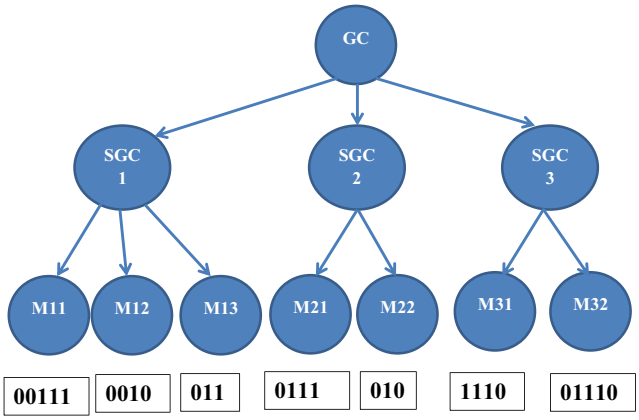

Fig. 3 UID generation

used to generate group key which is explained in the following steps:

1. GC randomly selects any four images.
2. GC clicks on the images in a sequential order with one click per image. The location where the GC clicks is a pass point of that image. GC generates four pass points for the corresponding four images it had randomly selected.
3. These pass points are distributed to each member and subgroup controller.

Pass point of the first image is considered as the base point which is used for further encryption and decryption of messages to provide secure communication. The four random images along with the generated pass points are used for generating the subgroup key. These images and pass points are distributed to each member in that particular subgroup.

The benefits of pass points are that it has a huge password space in comparison with alphanumeric passwords. This method of key generation increases the security level when compared to the existing technique. This graphical password [19, 20] can be easy to remember, provides protection from different denial of service attacks. Shoulder surfing technique deals with an attacker who does not require any technical skills to get the personal information of a victim instead a keen observation of the victims' surroundings and the typing pattern is sufficient for cracking the password.

3.3 Public-private key generation

Each member under subgroup is having public and private keys. These keys are used for one to one communication between members of the group. This key is generated based on elliptic curve cryptography. In ECC, public and private keys are generated as follows:

4. Create base point G. It is a pass point which was generated during GK generation phase.
5. Calculate a private key using Eq. (1)

$$PR_{i,j} = random(\,) \tag{1}$$

Calculate a public key using Eq. (2)

$$PU_{i,j} = G \times PR_{i,j} \tag{2}$$

where, PRi,j is a private key of jth member in a ith subgroup, PUi,j is a public key of jth member in a ith subgroup, random() is a random generation function. This key pair is used for one to one communication.

Example: If a numerical base point value taken from the image is 1,036,224,036 and the private key value is 946 then the resultant public key is 980,267,938,056 60,413.

3.4 Communication and authentication

The communication [21] begins once after generating all those mentioned keys. The communication steps are listed as follows:

6. If one of the members in a group needs to send a message m to other member, then request message for sending a message is sent to the GC.
7. A message is encoded and it is denoted as P_m.
8. A receiver should be an authorized person. The graphical password must be entered correctly which is already been distributed by GC and SGC.
9. First arrange the sequence of images and then click correct pass point value. Repeat the same step for sub group key. If it is successful then communication can takes place.
10. Secret key is produced through Eq. (3)

$$SK = PR_{i,j} \times PU_{i,k} \tag{3}$$

such that $j \neq k$, where $PR_{i,j}$ is a private key of j_{th} member in i_{th} subgroup and is the sender of the message, $PU_{i,k}$ is a public key of k_{th} member in i_{th} subgroup and is to establish the secret key.

GC chooses a random positive integer i and used this value to encrypt the message. The encrypted message is in Eq. (4) format

$$C_m = \{iG, P_m + iPU_{i,k}\} \tag{4}$$

11. This encrypted message is sent to the destination or receiver.

12. A receiver of a message has to decrypt it. Cipher text consists of two coordinates that are in point format. For decryption of the message, the first coordinate needs to be multiplied by receiver's private key $PR_{i,k}$ and then subtract it from second coordinate as shown in Eq. (5)

$$P_m + iPU_{i,k} - PR_{i,k(iG)} = P_m + i(PR_{i,k}G) - PR_{i,k}(iG) = P_m \quad (5)$$

Where P_m is the message sent by the sender and is received by the receiver. Hence, a receiver gets a message.

3.5 Rekeying

In this scheme, any member can join or leave a group at any time. Whenever a membership changes occur in a subgroup, rekeying is done. The GC maintains two databases. One database stores the details of the members who are all currently present in the group named as Present member Database (PMDB), another one is used to store a leaving member's details named as Leaving Member Database(LMDB). During rekeying only subgroup key of conforming subgroup is to be changed for maintaining forward and backward secrecy.

3.5.1 Leaving operation

Whenever a userr wishes to exit from a group, it sends a request to a GC. GC removes the data about that member and stores it in a leaving member database. After removing route, a subgroup key of that particular subgroup has to be changed in the same manner as discussed in the section 3.2.

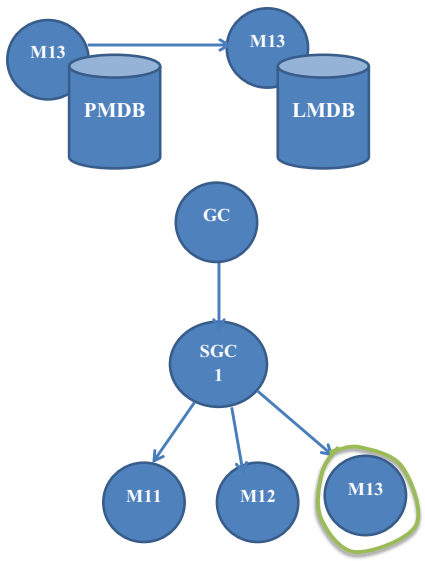

Fig. 4 Leaving operation

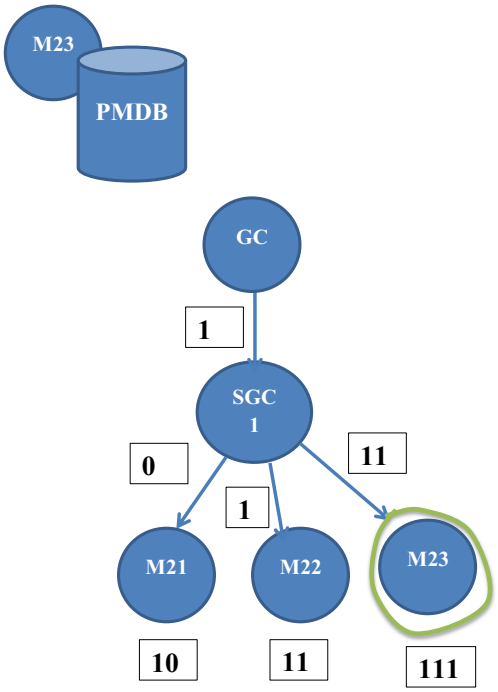

Fig. 5 Joining operation

In Fig. 4, Member 3 of SGC1 (M_{13}) wants to exit from a subgroup, the data about that member is removed from PMDB and is inserted into the LMDB. After leaving, SGC1 produces a new unique subgroup key and distributes it to rest of the members in that subgroup. If M_{13} wants to communicate with the group member, he/she can't communicate because of the changed subgroup key. But still group key is the same. Even M_{13} knows a group key he/she couldn't communicate because of unknown subgroup key. Therefore, M_{13} cannot read the further messages that are exchanged between that subgroup. Hence, it maintains forward secrecy.

3.5.2 Joining operation

Whenever a new user needs to enter a Sub Group, it transmits a request to a GC. GC generates the UID for that member and distributes it to the corresponding subgroup controller and SGC forward it to the respective member. After generating UID, GC sends it key value which is graphical password to that new member. SGC change its own key value and send it to a new member. A new member generates a public-private key pair of its own. These key generations performed based on

Table 1 Cost for communication

	Joint Event	Remove Event
OFTs	$log_2n + 1.0$	$log_2n + 1.0$
LKHs	$2log_2n$-1.0	log_2n
Proposed Scheme	1.0	1.0

Table 2 Cost for computation

	Joint Event	Remove Event
OFTs	$log_2n + 1$	$log_2n + 1$
LKHs	$2log_2n$-1	$2log_2n$
Proposed Scheme	0.9	0.99

methods described in section 3. Then GC inserts the data about that member into PMDB. Now, a new member can communicate with any other member in that group. But this new member couldn't read the messages which were previously shared between the members.

A new user M_{23} wants to enter a group under subgroup 2 (SGC2) where i = 2 represents SGC2 and j = 3 represents 3rd member M which is shown in Fig. 5. Initially it sends a join request to GC. The GC accepts a join request based on the subscription span value. Then, UID is generated with the help of modified Huffman coding as defined in the section 3. Then SGC2 regenerate its own key based on subgroup key generation discussed in section 3.2. The new member's details are inserted into PMDB. Now, a new member can communicate with other members in that subgroup. Hence, it maintains the backward secrecy.

4 Analysis

In the proposed scheme, group key is static. On every occasion of group changes the sub group key will be altered. The cost of computation of group key is 1 initially. It is nil in the further modification of group since it is static. There are no means of communication happening while sharing the group key to the members of the group. Hence, the cost of communication is reduced. Since the key is a graphical password, changing the image sequence and getting new pass points acts as a new base point for generating the sub group key and the process continues. Hence, it continues in the forward and backward motion with secrecy and also reduces computation and communication cost. Table 1 and Table 2 explains the comparison among current and proposed system for communication cost and computation cost respectively.

5 Conclusion

Secure key management system for multicast network provides much more efficient communication between group members with the use of graphical password instead of textual password. The secret of the user can be protected from any kind of malicious attack using the proposed graphical approach with low cost and attains great benefits by using onward secrecy and recessive secrecies, key liberation, scalability, Security, etc. GK remains same for the entire process. As a result of static group key, the computation and communication cost are reduced. Proactive secret sharing structure improves the security level of communication. Encryption and decryption process can be performed with a smaller key size. This scheme provides more security, efficient key management with smaller key size when compared to the literatures.

References

1. Srinivasan R, Vaidehi V, Rajaraman R, Kanagaraj S (2010) Secure group key management scheme for multicast networks. Int J Netw Sec 11(1):33–38
2. Real User Corporation: Passfaces. www.passfaces.com
3. Dhamija R, Perrig A (2000)Deja vu: a user study using images for authentication. Proc 9th USENIX Sec Sym
4. Mingyan L, Poovendran R, Berenstein C (2002) Design of Secure Multicast key Management Schemes with Communication Budget Constraint. IEEE Commun Lett 6(3):108–110. https://doi.org/10.1109/4234.991148
5. Pitipatana S, Nirwan A (2007) Elliptic curve cryptosystem-based group key Management for Secure Group Communications, Proc IEEE Military Commun Conf Orlando, USA: 1–6
6. Sharma S, Rama Krishna C (2015) An efficient distributed group key management using hierarchical approach with elliptic curve cryptography. Proc IEEE Int Conf Comput Intell Commun Technol Ghaziabad U.P, India 116:687–693. https://doi.org/10.1109/CICT.2015
7. E. Munivel, J. Lokesh (2008) Design of Secure Group key Management Scheme for multicast networks using number theory. Proc Int Conf Comput Intell Modell Control Autom Vienna, Austria. doi:https://doi.org/10.1109/CIMCA.2008. 29, pp.124–129
8. Jabeen Begum S, Purusothaman T (2011) A new scalable and reliable cost effective key agreement protocol for secure group communication. J Comput Sci 7(3):328–340
9. Li S, Wu Y (2010) A survey on key management for multicast. Proc Second Int Conf Inform Technol Comput Sci Vienna, Austria 82: 309–312. https://doi.org/10.1109/ITCS.2010
10. Rafaeli S, Hutchison D (2003) A survey of key management for secure group communication. ACM Comput Surv 35(3):309–329. https://doi.org/10.1145/937503.937506
11. Srinivasan T, Sathish S, Vijay Kumar R, Vijayender MVB (2006) A hybrid scalable group key management approach for large dynamic multicast networks. Proc Sixth IEEE International Conf. on Computer and Information Technology, Dhaka, Bangladesh. https://doi.org/10.1109/CIT.2006.9
12. Ilango S, Thomas J (2004) Group key management utilizing Huffman and Petrick based approaches. Proc Int Conf Inform Technol: Coding Comput Las Vegas, USA. https://doi.org/10.1109/ITCC.2004.1286664
13. Nasreldin Rasslan MM, Dakroury HY, Aslan HK (2009) A new secure multicast key distribution protocol using combinatorial Boolean approach. Int J Netw Sec 8(1):75–89
14. Jancy Rani D, Sabarinathan P (2016) Security based service key Management for Multiple Group. Int J Innov Res Comput Commun Eng 4(1):556–560. https://doi.org/10.15680/IJIRCCE.2016.0401126

15. A. Herzberg, S. Jarecki, H. Krawczyk, Yung M (1995) proactive secret sharing or how to COpe with perpetual leakage, Proc 15th Annual International Cryptology Conference Adv Cryptol, Springer-Verlag, California, USA: 339–352
16. Walanjkar DD, Nandedkar V (2014) User authentication using graphical password scheme: a more secure approach using Mobile Interface. Int J Innov Res Comput Commun Eng 2(12): 7329–7335. https://doi.org/10.15680/ijircce.2014.0212053
17. Keerthana R, SaravanaKumar NM (2014) A cost effective multicast key management scheme for secure group communication. Int J Innov Res Comput Commun Eng 2(1):1177–1183
18. Mythili GM, SaravanaKumar NM (2014) Dynamic architecture for scalable and proficient group key management. Int J Innov Res Comput Commun Eng 2(1):1177–1183
19. Khandelwal A, Singh S, Satnalika N (2010) User authentication by secured graphical password implementation. Int J Comput Applic 1(25):100–104. https://doi.org/10.5120/449-751
20. Moraskar V, Jaikalyani S, Saiyyed M, Gurnani J, Pendke K (2014) Cued click point technique for graphical password authentication. Int J Comput Sci Mobile Comput 3(1):166–172
21. Widenbeck S, Waters J, Birget J, Brodskiy A, Memon N (2005) Authentication using Graphical Passwords: Basic Results. Proc Sym Usable Privacy Security, New York, USA:1–12. doi:https://doi.org/10.1145/1073001.1073002