Volume No:3, Issue No:2 (July-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

A Secure Group Key Agreement with Local Connectivity Using Multicast Key Management

Subba Reddy Kamireddy
M.Tech,
Dept of CSE,
Swarnandhra Institute of Engineering and Technology, JNTUK, Narsapur, W.G, A.P, India.

Anand Kumar Deva
Assistant Professor,
Dept of CSE,
Swarnandhra Institute of Engineering and Technology, JNTUK, Narsapur, W.G, A.P, India.

Dr. T. Murali Mohan, Ph.D
Associative Professor & HOD
Dept. of CSE,
Swarnandhra Institute of Engineering and Technology, JNTUK, Narsapur, W.G, A.P, India.

I. ABSTRACT:

In this paper, we study Group key Agreement which mean multiple parties want to create a common secret key to be used to exchange information securely. The group key agreement with an arbitrary connectivity graph, where each user is only aware of his neighbor and has no information about the existence of other users. Further, he has no information about the network topology. We implement the existing system with more efficient manner and provide a multicast key generation protocol. We replace the Diffie-Hellman key exchange protocol by a new multicast key exchange protocol that can work with One-to-One and One-to-Many functionality. We also tend to implement a strong symmetric key encryption for improving file security in the system.

KEYWORDS:

Multicast Exchange Protocol, Group Key Agreement.

II.INTRODUCTION:

In scattered framework, gathering key declaration tradition expects an essential part. They are expected to give a social occasion of customers with a typical mystery key to such an extent that the customers can securely talk with each other over an open framework. Gathering key comprehension implies various social occasions need to make an average mystery key to be used to exchange information securely.

We consider the social affair key simultaneousness with a self-emphatic system chart, where each customer is recently aware of his nearest and has no information about the nearness of various customers. Facilitate, he has no information about the framework topology. In our issue, there is no mean energy to instate customers. Each of them can be instated self-governing using PKI (open key foundation). A social event key affirmation for this setting is uncommonly appropriate for applications, for instance, an interpersonal association. Under our setting, we create two profitable idly secure traditions.

We moreover exhibit bring down cutoff points on the round Complexity which evidence that our traditions are round capable. In extraordinarily selected framework, the customers are commonly versatile. The social affair part is not known early and the customers may join and leave the get-together a great part of the time. In such circumstances, component gathering key comprehension traditions are required. Such arranges must ensure that the social event session key over after get-together part changing with the end goal that subsequent session keys are protected from the leaving people and past session keys are protected from the joining people. There are especially different component gathering key comprehension traditions. Customer security infers that any leaving part room a get-together can't create new assembling and joining part into a social affair can't discover heretofore used assembling key.

Volume No:3, Issue No:2 (July-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In this errand we complete the present structure with extra time gainful way and give a multicast key time server which is typical in future expansion by current makers. We supplant the Diffie-Hellman key exchange tradition by another multicast key exchange tradition that can work with adjusted and one to various values. We in like manner have a tendency to execute an in number symmetric encryption for improving record security in the system.

III. SCOPE:

In Social networking sites group key agreement plays a vital role for secure distribution of files. In this we make two passively secure protocols with contractiveness and proved lower bounds with round efficient. At last we make an actively secure protocol from passive one. In this presentation we did not consider updating of group key more efficiently than running protocol according to user memberships.

IV. EXISTING SYSTEM:

Key pre-conveyance framework (KPS) (a.k.a. no interactive gathering appropriation framework) can be viewed as a non-intelligent gathering key exchange. For this situation, the mutual key of a given gathering is settled after the setup. In the event that a gathering is overhauled, then the mass key changes to the common key of the new amass. The disadvantage of KPS is that the client key size is combinatorial huge in the aggregate number of clients (if the framework is genuinely secure). Another downside is that the gathering key of guaranteed gather can't be changed regardless of the possibility that it is spilled surprisingly (e.g., cryptanalysis of figure writings bearing this key). The key size issue might be overcome if a calculationally secure framework is utilized, while the key spillage issue is difficult. Assist, calculationally secure KPS is just familiar for the two party case and the three-party case KPS with a gathering size more noteworthy than 3 is still open.

The client key size is combinatorial substantial in the aggregate number of clients (if the framework is unequivocally secure).The assemble key of a given gathering can't be changed regardless of the possibility that it is spilled suddenly.

V. Proposed System:

The gathering key concurrence with a discretionary network diagram, where every client is just mindful of his nearest and has no data about the presence of different clients. Facilitate, he has no data about the system topology. Under this setting, a client does not have to believe a client who is not his neighbor. In this manner, in the event that one is instated utilizing PKI, then he require not trust or recollect public keys of clients past his nearest. In proposed system we implement the existing system with more time efficient manner and provide a multicast key generation server which is expected in future scope by current authors. We replace the Diffie Hellman key exchange protocol by a new multicast key exchange protocol that can work with one-to-one and one-to- many functionality. We also tend to implement a strong symmetric encryption for improving file security in the system.

Advantages:

To redesign the gathering key more effectively than just running the convention once more, when client enrollments are evolving. Two latently secure conventions with responsible and demonstrated lower limits on a round intricacy, exhibiting that our conventions are round proficient.

VI. PRELIMINARIES:

Notations: We will need to follow these notions.

For a set S, x ←S samples x from S evenly randomly;

Function: N→R is negligible if for any polynomial $p(x)=\lim_{n\to\infty}\mu(n)p(n) = 0$.

X is Alice, Y is bob ,a is common prime key.

$X = P^x \bmod(a)$ is the a (prime values), x which indicatives secret integer of alice, x_i which indicatives public key of alice,Pprimitive root.

Volume No:3, Issue No:2 (July-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Now Alice compute, $(Y)^{x}{}_{i}$mod(a)
Now he is getting one value that is k
Y = P^{y}mod(a) is the a (prime values) , y which indicatives secret integer of bob, y_i which indicatives public key of bob. P primitive root.
Now Bob compute, $(X)^{y}{}_{i}$mod(a)
Now he is getting one value that is k.
Alice and Bob now share a secret (the value k)

Indistinguishability:

Two ensembles are indistinguishable if no efficient algorithm can tell them apart. This notion was first proposed by Goldwasser and Micali in case of encryption. Generally, it was due to Yao[15].
Definition 1: Ensembles $X = \{X_\alpha\}_{\alpha \geq 1}$ and $Y = \{Y_\alpha\}_{\alpha \geq 1}$ are indistinguishable if for any Diffie- algorithm D, $|Pr[D(X_\alpha) = 1] - Pr[D(Y_\alpha) = 1]|$ is negligible.
In a cryptographic system, α usually is the security parameter and implicitly defined. For example, in a RSA system, α is the bit length of the modulus N.

Decisional Diffie-Hellman Assumption:

Consider a (multiplicative) cyclic group G of order p, and with generator g. The DDH assumption states that, given g^x and g^y for uniformly and independently chosen x,y€ Z_p the value g^{xy} looks like a random element in G. The decisional Diffie-Hellman assumption is as follows.

Definition 2: The decisional Diffie-Hellman assumption (DDH) holds if (g^x, g^y, g^{xy}) where x and y are randomly and independently chosen from Z_p (g^x; g^y; g^z) where x,yand z are randomly and independently chosen from Z_p The subgroup of k th residues modulo a prime a, where (a-1)/k is also a large prime (also called a Schnorr group). For the case of k=constant , this corresponds to the group of quadratic residues modulo a safe prime. The following lemma can be easily proved by a hybrid reduction and it appeared in[16].Lemma 1: Let n to N.

Then, under the DDH Assumption, $\{g^{ai,aj}\ 1 \_ i < j \_ n\} \cap \{g, g^{a1},\ldots, g^{an}\}$ And $\{g^{aij} \mid 1 \leq i < j \leq n\} \cap \{g, g^{a1},\ldots, g^{an}\}$ Indistinguishable, where a_{ij} (1 _ i < j _ n) and $a_{1\ldots\ldots}a_n$;are all uniformly random from Z_q:

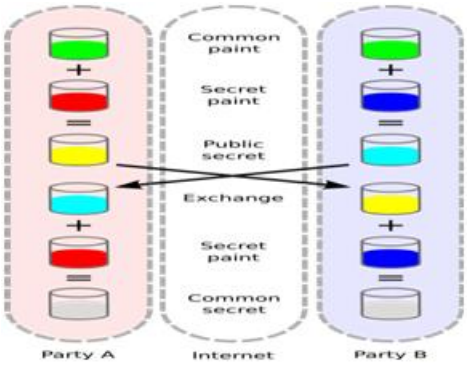

FIG: - Diffie- hellman Key Exchange

Algorithms:

Multicast key Management protocol Algorithm

(Active User)

Stage one.

0. Each i € V takes $a_i \rightarrow Z_q$ and sets $A_i = g_a i$:
1. Each leaf user s in G (i.e., $N_s = x$) sets $A_s i = 1$ and sends ($A_s i$, A_s) to i:
2. [**Loop**] Each V does the following.
For i € N, if user has received (A_i ,A_j) from each j € N_n and did not send (A_i , A) to i, then he computes A_i = j €N_n and sends (A_i , A_j) to i.
3. Each user continues stage 2 until he has sent (A_i , A) to user i for each i 2 N`, in which case, he proceeds to Stage two.

Stage two.

1. Each leaf user s (i.e., $N_s = x$) computes $L_s i$ =A and sends $C_s i = E_s i\ (L_s i)$ to user i:
2. [**Loop**] Each V does the following.For i € N, if user has received Cj fromeach j € N and did not send C_i toi then he decrypts $L_j = D_j\ (C_j)$, defines
L_i = (j€N_n f(x)L),(j€N A_j)a and sends $C_i = E\ (L_i)$ to user i.
3. Each user continues stag 2 until he has sent C_i to user i for each i € N, in which case, he proceeds to Stage three.

Volume No:3, Issue No:2 (July-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Stage three (group key derivation).

Upon C_s for all S€ N, user decrypts$L_s = D_s (C_s)$ (if not done before) andcalculates group key $s_k = Q_s$€ $N(L_s , A_s) = Q (u.v)=V(g_a)$.

(Passive user)

Stage one.

Each user (i, v) takes a_i ; Z_q; c_i, f(X)and defines Ai = g_ai Then, user i sends $A_i$to his nearest N_i and receives A_j from each j € N

Stage two.

1. Each leaf user s (with N_s = X) computesc_si = c_i and sends C_si = E_si (c_si) to i:
2. [**Loop**] Each V does the following.

For i € N, if user has received Cj from allj € N_n X and did not send C_i thenhe decrypts C_j= $D_j(C_j)$, computes C_i =$C_i(C_j$€N_n f(x) C_s(i)) and sends C_i = E_i (c_i)to user i:

3. Each user continues stag 2 until he has sent C_i to each i € Nin which case, he proceeds to Stage three.

VII. RESULT GRAPH

In this screen which represents the graph between Total Group Members and Available Group Members Details.

VIII. CONCLUSION:

We mulled over a gathering key understanding issue, where a client is just mindful of his nearest while the network chart is subjective. What's more, clients are instated totally autonomous of one another. A gathering key assertion in this setting is extremely suitable for applications, for example, informal communities.

We review distinctive arrangements proposed in this space and reasoned that much work is should have been be done in this understanding conventions. We further propose a voting based convention plan for better protection and security in gathering based situations.

IX. REFERENCES:

1. Shaoquanjiang,"Group key agreement protocol with local connectivity" Dependable and Secure Computing, IEEE Transactions on (Volume:PP ,Issue: 99),03 February 2015.

2. Zongyu Song, PengfeiCai, Jie Yang ,"Group key agreement with efficient communication for ad hoc networks" JOURNAL OF SOFTWARE, VOL. 8, NO.10, OCTOBER 2013.

3. Anurag Singh Tomar, Gaurav Kumar Tak, Manmohan Sharma"Secure Group Key Agreement with Node Authentication", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 4, April 2014.

4. k.kumar,j. Nafeesa Begum , Dr V. Sumathy, "Novel Approach towards cost Effective Region Based Key Agreement Protocol for secure Group Communication" in International Journal of Computer and Information Security, vol.8,No. 2,2010.

5. N. Renugadevi ,C. Mala "Ternary Tree BaseGroup Key Agreement for Cognitive Radio MANETs" in I.J. Computer Network and Information Security, 2014, 10, 24-31 Published Online September 2014 in MECS

6. Reddi Siva Ranjani, D.LalithaBhaskari, P. S.Avadhani, "An Extended Identity Based Authenticated Asymmetric Group Key Agreement Protocol", in International Journal of Network

Security, Vol.17, No.5, PP.510-516, Sept. 2015.

7. TrishnaPanse, Vivek Kapoor, PrashantPanse, "A Review on Key Agreement Protocols used in Bluetooth Standard and Security Vulnerabilities in Bluetooth Transmission", in International Journal of Information and Communication Technology Research, Volume 2 No. 3, March 2012.
8. M. Swetha, L. Haritha, "Review on Group Key Agreement Protocol", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 10, December- 2012.
9. Abhimanyu Kumar, SachinTripathi, "Ternary Tree based Group Key Agreement Protocol Over Elliptic Curve for Dynamic Group" ,in International Journal of Computer Applications (0975 – 8887) Volume 86 – No 7, January 2104
10. Mahdi Aiash, GlenfordMapp and AboubakerLasebae, "A Survey on Authentication and Key Agreement Protocols in Heterogeneous Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July 2012.
11. K. Kumar, J. Nafeesa Begum, Dr.V. Sumathy, "A Novel Approach towards Cost Effective Region-Based Group Key Agreement Protocol for Secure Group Communication",in(IJCSIS) International
12. Journal of Computer Science and Information Security, Vol. 8, No. 2, 2010.Amr Farouk, Mohamed M. Fouad and Ahmed A. Abdelhafez, "Analysis and Improvement of Pairing-Free Certificate-Less Two-Party Authenticated Key Agreement Protocol for Grid Computing", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1, February 2014.
13. (Eurocrypt'02), vol. 2332, pp. 321-336, 2002.
14. Chengzhe Lai, Hui Li, Rongxing Lu, Xuemin(Sherman) Shen, "A secure and efficient group authentication and key agreement protocol for LTE networks" , Computer Networks 57 (2013) 3492.