International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 2 March-April 2017 p-ISSN: 2394-8280

SECURITY USER DATA IN LOCAL CONNECTIVITY USING MULTICAST KEY AGREEMENT

Pallavi Wadkar[1], Prof. Sonal Honale[2]
Dept. Of Computer Science And Engg.,Abha Gaikwad College of Engineering Nagpur

Abstract: In this paper, we study Group key agreement means 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 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. Through experimentation we find the time required for join and leave part as well as time required for encryption is much less as compared to existing methodologies.

I. INTRODUCTION

In dispersed system, I gathering key assention convention assumes a vital part. They are intended to give a gathering of clients with a common mystery key such that the clients can safely speak with one another over an open system. Gathering key understanding means numerous gatherings need to make a typical mystery key to be utilized to trade data safely. We think about the gathering key concurrence with a self-assertive network diagram, where every client is just mindful of his neighbors and has no data about the presence of different clients. Further, he has no data about the system topology.

In our issue, there is no focal power to instate clients. Each of them can be instated autonomously utilizing PKI. A gathering key assention for this setting is exceptionally suitable for applications, for example, an interpersonal organization. Under our setting, we develop two productive latently secure conventions. We likewise demonstrate lower limits on the round Complexity which shows that our conventions are round proficient.

In specially appointed system, the clients are typically portable. The gathering part is not known ahead of time and the clients may join and leave the gathering much of the time. In such situations, element gathering key understanding conventions are needed. Such plans must guarantee that the gathering session key overhauls upon gathering part changing such that consequent session keys are shielded from the leaving individuals and past session keys are shielded from the joining individuals. There are very much various element gathering key understanding conventions. Client security implies that any leaving part from a gathering can't produce new gathering and joining part into a gathering can't find beforehand utilized gathering key.In this task we actualize the current framework with additional time productive way and give a multicast key era server which is normal in future extension by current creators. We supplant the Diffie Hellman key trade convention by another multicast key trade convention that can work with balanced and one to numerous usefulness. We likewise tend to execute an in number symmetric encryption for enhancing document security in the framework.

II. RELATED WORK

In this paper, a gathering key understanding issue where a client is just mindful of his neighbors while the network diagram is discretionary. In our issue, there is no unified instatement for clients. A gathering key concurrence with these elements is extremely suitable for informal communities. Under our setting, we develop two proficient conventions with detached security [1].

In dispersed system, gathering key assention convention assumes a vital part. They are intended to give a gathering of clients with a common mystery key such that the clients can safely speak with one another over an open system. Gathering key understanding means numerous gatherings need to make a typical mystery key to be utilized to trade data safely. We think about the gathering key concurrence with a self-assertive network diagram, where every client is just mindful of his neighbors and has no data about the presence of different clients. Further, he has no data about the system topology. In our issue, there is no focal power to instate clients. Each of them can be instated autonomously utilizing PKI. [2]

In this paper, an element validated gathering key assertion convention is exhibited utilizing blending for impromptu systems. In Join calculation, the quantity of transmitted messages does not increment with the quantity of all gathering individuals, which makes the convention more functional. The convention is provably secure. Its security is demonstrated under Decisional Bilinear Diffie-Hellman supposition. The convention likewise gives numerous different securities property [3]

In this paper, gathering key concurrence with hub confirmation plan has been proposed. It's a changed form which consolidates the components and benefits of both Flexible Robust Group Key Agreement and additionally Efficient Authentication Protocol for Virtual Subnet convention. The fundamental point of preference of proposed plan is that it dispenses with the need to send the different parameters for verification and additionally gathering key commitment [3]. This paper addresses a fascinating security issue in remote specially appointed system: the dynamic Group key Agreement key foundation. For secure gathering correspondence in Ad hoc system, a gathering key shared by all part. In this paper creator proposed a novel secure versatile and powerful Region-based gathering key understanding convention for Ad hoc system [6].

A Group Key Agreement (GKA) convention is an instrument to set up a cryptographic key for a gathering of members in light of every one's commitment, over an open system. The key, along these lines inferred, can be utilized to set up a protected channel between the members. In this paper, Author display a straightforward, secure and productive GKA convention appropriate to element impromptu systems. We additionally present consequences of our usage of the convention in a model application [7].

This paper exhibits an effective contributory gathering key understanding convention for secure correspondence between the lightweight little gadgets in subjective radio portable specially appointed systems. A Ternary tree based Group ECDH.2 (TGECDH.2) convention that uses a cluster rekeying calculation amid enrollment change is proposed in this paper. This ternary tree is an adjusted key tree in which proper insertion point is chosen for the joining individuals amid rekeying operation. TGECDH.2 joins the computational effectiveness of ECDH convention and [8].

III. PROPOSED APPROACH

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. The proposed work is planned to be carried out in the following manner:

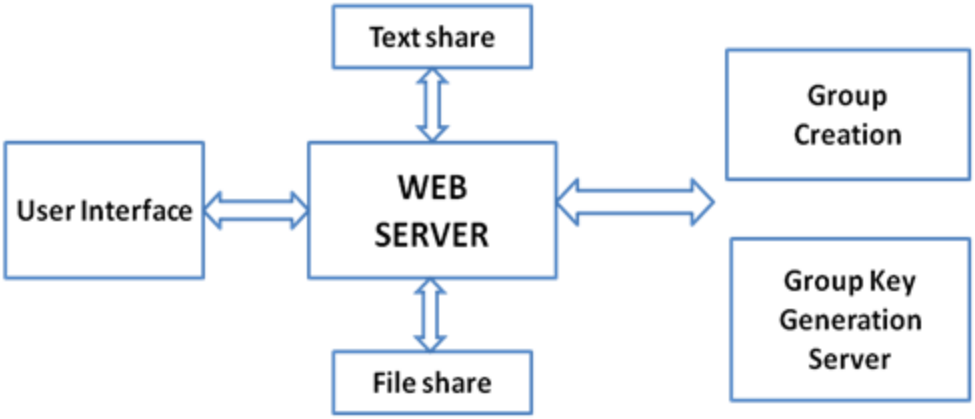
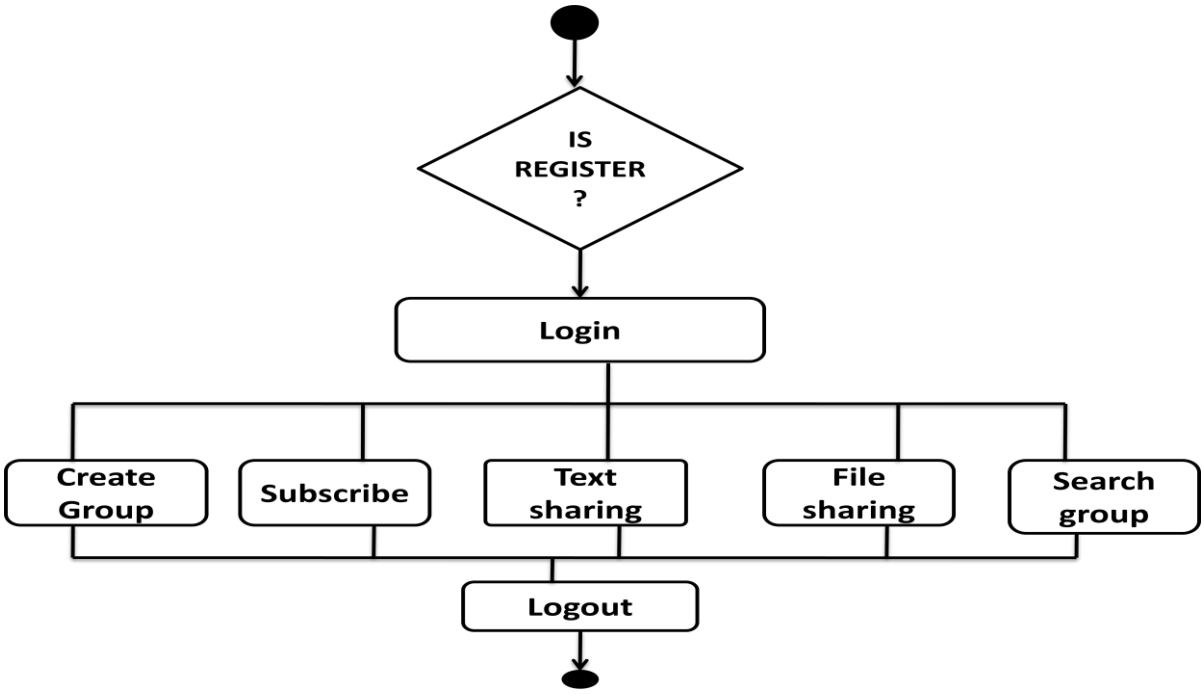


Fig: System Architecture of group key agreement

FLOWCHART:



IV. METHODOLOGY

MODULES

- **Group based data sharing web Application**
  Nowadays, group oriented applications are very popular and can be divided into one-to-many, few-to-many, and any-to-any applications. Among these, we are interested in any to any applications. Usually this kind of application, for example, video conference, is collaborative and such collaborative applications needs peer group underlying. This group also requires rich communication semantics and tighter control of members and put emphasis on reliability and security.
  We will be developing web based application that will provide group chat and file sharing services.
- **Data Encryption**
  The data to be share will be encrypted using AES Algorithm .the key will be generated using key generation server.

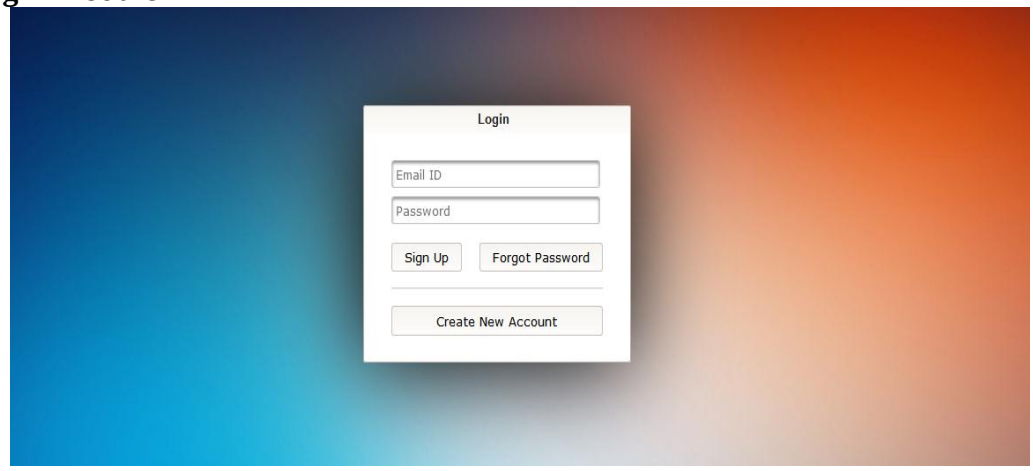
- **File Sharing**
  Data to be share will be in form of text or multimedia file.
- **Rekeying**
  Key management is a building block for all other cryptographic and secure applications.
  Whenever a user joins or leaves a group the multicast key server will generates a key and provide to all user of respective group.
- **Majority based voting scheme implementation**
  Whenever a user subscribe to some group the majority based voting protocol which will decide whether to approve or rejected user requested based on majority group.

Group Key Agreement Algorithm

1. Each group member contributes its (equal) share to the group key, which is computed as a function of all shares of current group members.
2. This share is secret (private to each group member) and is never revealed.
3. As the group grows, new members' shares are factored into the group key but old members' shares remain unchanged.
4. As the group shrinks, departing members' shares are removed from the new key and at least one remaining member changes its share
5. Current group members' shares are modeled as leaf nodes in a binary tree
6. Each link (edge) in the tree is labeled f (k) where k is the value of the node below the link
7. Each non-leaf node is labeled f (kl kr) where kl and kr are the labels of the left and right child node, respectively
8. The particular function f () used in our protocols is modular exponentiation in prime-order groups, i.e., f (k) = k (mod p)
9. Computing the labeled value of a non-leaf node requires the knowledge of the value of one of the two child nodes and the value of the other incident link (i.e., link value emanating from the other child node).
10. All protocol messages are signed by the sender. (We use AES for this purpose).

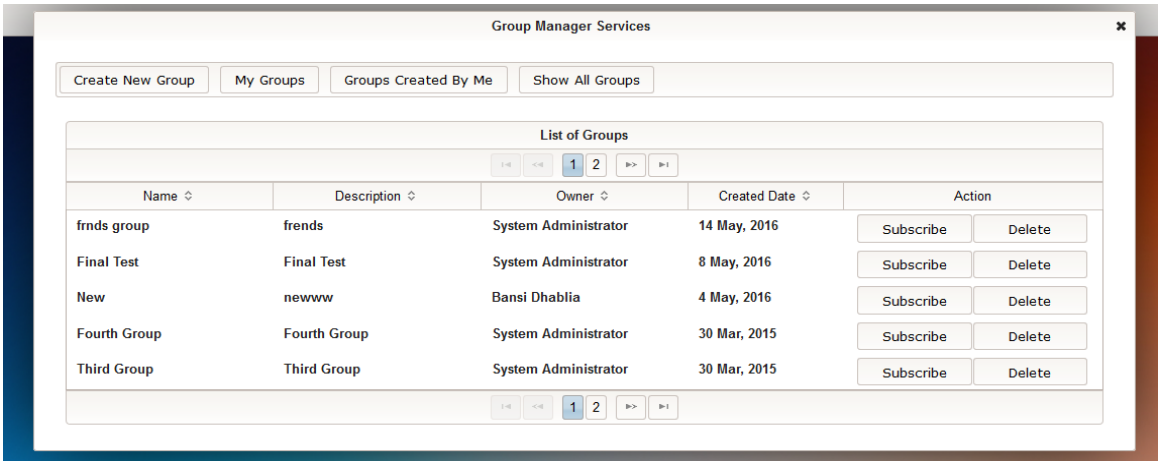
DESIGN WORK

- **Login Module**

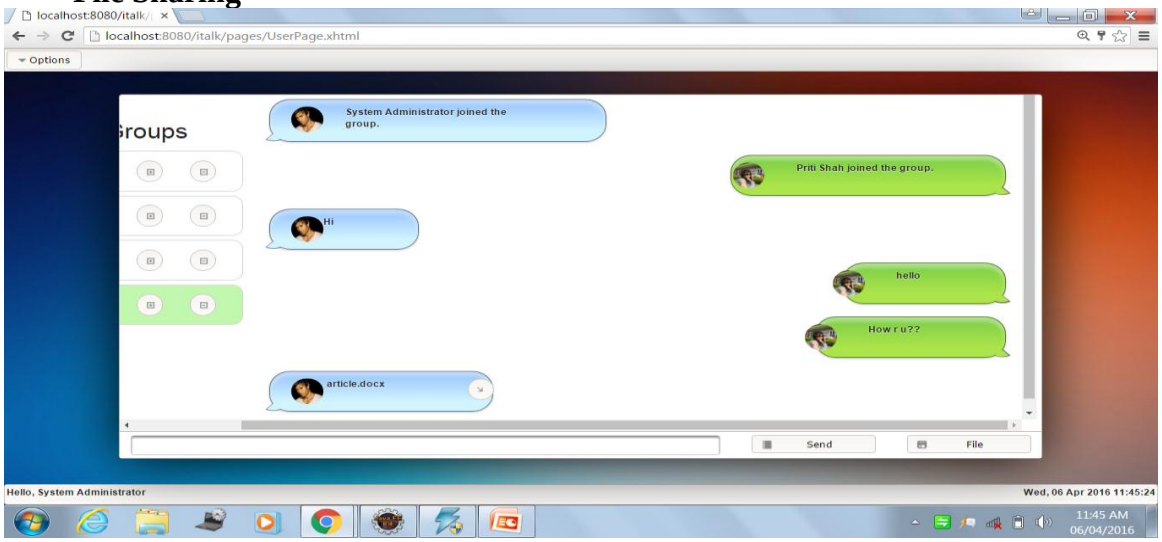


- ❑ **Data Encryption**
- **Group Manager Services**

e-ISSN: 2394-8299
p-ISSN: 2394-8280

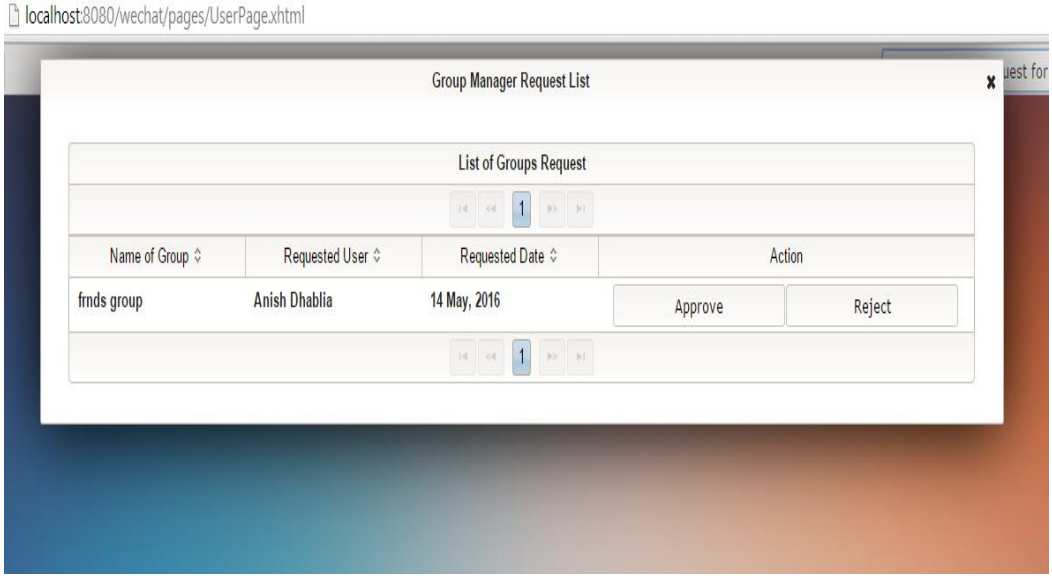


- **File Sharing**

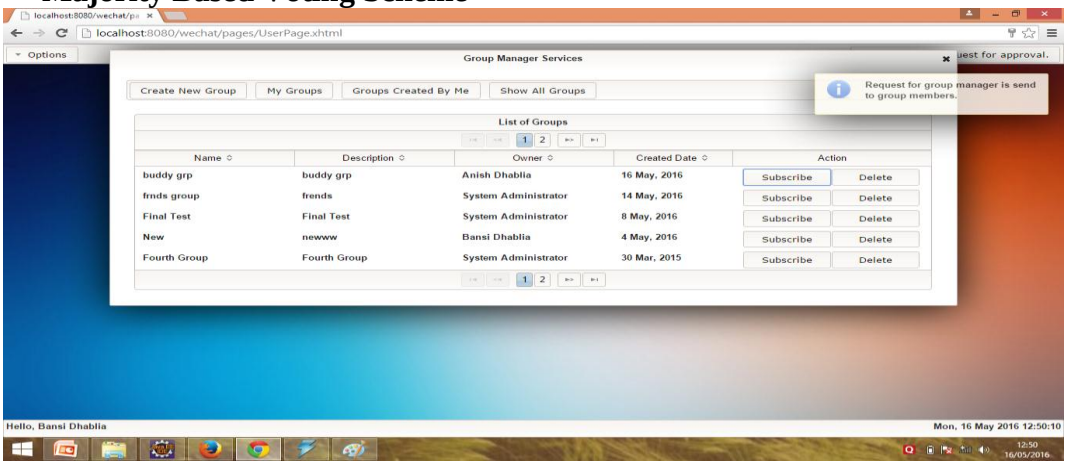


- **REKEYING**

Group Manager Request service



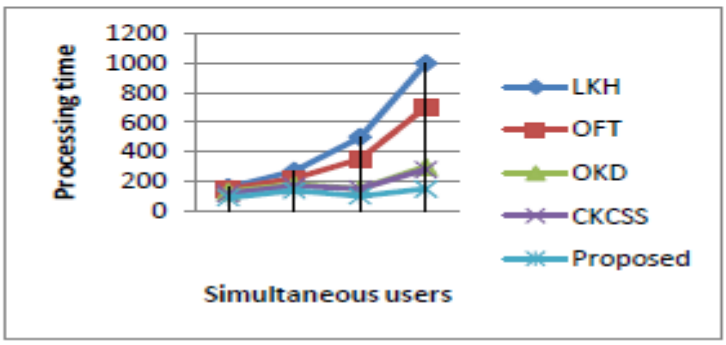
- **Majority Based Voting Scheme**



RESULTS AND DISCUSSION

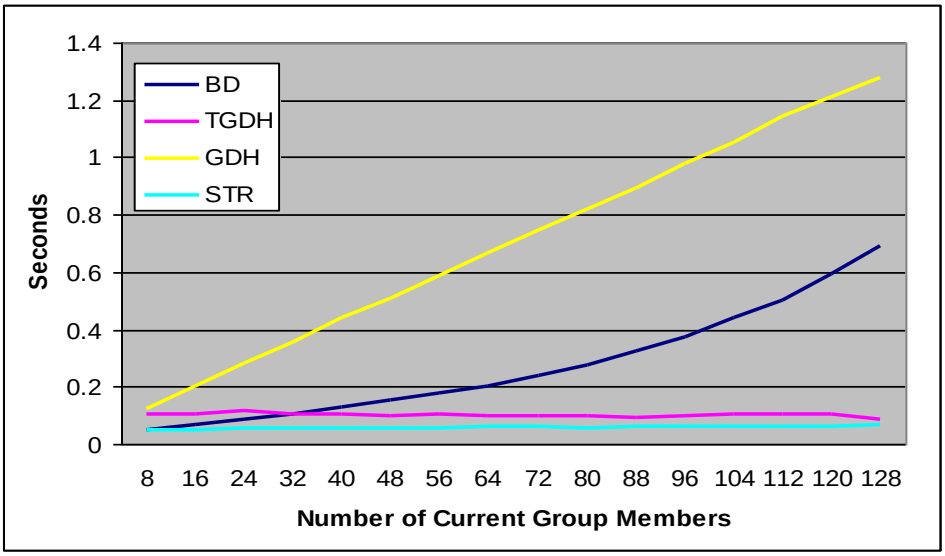
Comparisons:

We presented a comparison that shows the complexity of the group generation and the processing time of the process.Table1.The comparisons of key generation in simultaneous join or leave operations are shown below.

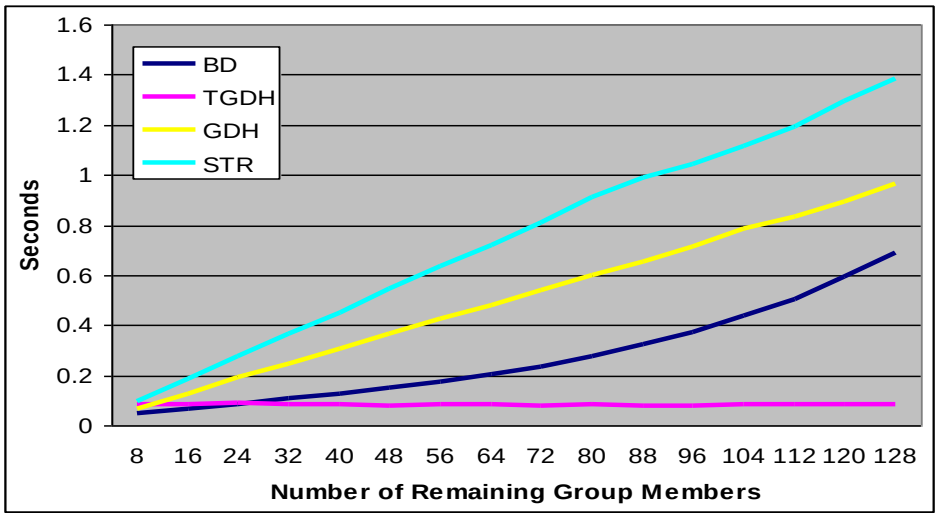


Protocol	Join	Leave
LKH	$m\log_2 n$	$m\log_2 n$
OFT	$m\log_2 n$	$m\log_2 n$
OKD	$m\log_2 n$	$m\log_2 n$
CKCS	m+1	1
PROPOSED	O(n)	O(n)

- Computational Cost (Join and Leave)



TGDH: Joining node is near to root due to random tree



V. CONCLUSION AND FUTURE ENHANCEMENT

We mulled over a gathering key understanding issue, where a client is just mindful of his neighbors 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.

In future one can either propose, improving fast decision making using timing based protocol. And providing individual chat rooms for users. And the project can also be extended by implementing some methodology in mobile app platforms.

REFERENCES

[1] Shaoquan jiang,"Group key agreement protocol with local connectivity" Dependable and Secure Computing, IEEE Transactions on (Volume:PP , Issue: 99),03 February 2015.
[2] Shahela A Khan,Prof. Dhananjay M. Sable "Survey on Security User Data in Local Connectivity Using Multicast Key Agreement" in International Journal on Recent and Innovation Trends in Computing and Communication , Volume: 3 Issue: 10
[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] 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.
[6] N. Renugadevi ,C. Mala "Ternary Tree Based Group Key Agreement for Cognitive Radio MANETs" in *I.J. Computer Network and Information Security*, 2014, 10, 24-31 Published Online September 2014 in MECS
[7] 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.
[8] Reddi Siva Ranjani, D. Lalitha Bhaskari, 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.
[9] Trishna Panse, Vivek Kapoor, Prashant Panse, "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.
[10] M. Swetha, L. Haritha, "Review on Group Key Agreement Protocol", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 10, December- 2012.
[11] Abhimanyu Kumar, Sachin Tripathi, "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 2014.*
[12] Mahdi Aiash, Glenford Mapp and Aboubaker Lasebae, "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.