[Awachat, 3(6): June 2016]

ISSN 2348 – 8034
Impact Factor-4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

DATA SECURITY AND PRIVACY IN GROUP BASED ENVIRONMENT USING MULICAST KEY MANAGEMENT AND MAJORITY BASED VOTING PROTOCOL

Ms. Sharayu Awachat[*1] and Prof. Jayant Adhikari[2]

[*1,2]TGPCET Mohgoan Nagpur

ABSTRACT

In this paper, we think about Group key assertion implies numerous gatherings need to make a typical mystery key to be utilized to trade data safely. The gathering key concurrence with a subjective network chart, where every client is just mindful of his neighbor and has no data about the presence of different clients. Further, he has no data about the system topology. We actualize the current framework with additional time proficient way and give a multicast key era server which is normal in future degree 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 additionally tend to actualize a solid symmetric encryption for enhancing record security in the framework.

Keywords: *Data security, Key management, Voting protocol etc.*

I. INTRODUCTION

In scattered framework, I assembling key assertion tradition expect an imperative part. They are proposed to give a social event of customers with a typical puzzle key such that the customers can securely talk with each other over an open framework. Gathering key comprehension implies various social affairs need to make an average puzzle key to be used to exchange information securely. We consider the get-together key simultaneousness with a self-confident system outline, where each customer is only aware of his neighbors and has no information about the nearness of various customers. Further, he has no information about the framework topology.

In our issue, there is no central energy to instate customers. Each of them can be instated self-ruling using PKI. A social event key assertion for this setting is particularly reasonable for applications, for instance, an interpersonal association. Under our setting, we create two beneficial inactively secure traditions. We in like manner exhibit lower limits on the round Complexity which demonstrates that our traditions are round capable.

In exceptionally delegated framework, the customers are regularly convenient. The social occasion 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 upgrades after get-together part changing such that resulting session keys are protected from the leaving people and past session keys are protected from the joining people. There are particularly different component gathering key comprehension traditions. Customer security infers that any leaving part from a get-together can't deliver new assembling and joining part into a social occasion can't discover previously used assembling key. In this undertaking we realize the present structure with extra time gainful way and give a multicast key period server which is ordinary in future augmentation 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 convenience. We similarly have a tendency to execute an in number symmetric encryption for upgrading record security in the system.

II. RELATED WORK

In this paper, a get-together key comprehension issue where a customer is only aware of his neighbors while the system outline is optional. In our issue, there is no brought together instatement for customers. A social occasion key simultaneousness with these components is to a great degree reasonable for casual groups. Under our setting, we create two capable traditions with separated security [1].

In scattered framework, gathering key assertion tradition accept a fundamental part. They are expected to give a social event of customers with a typical puzzle key such that the customers can securely talk with each other over an open framework. Gathering key comprehension implies various social events need to make a normal riddle key to be

ISSN 2348 – 8034
Impact Factor-4.022

used to exchange information securely. We consider the social event key simultaneousness with a self-confident system outline, where each customer is only aware of his neighbors and has no information about the nearness of various customers. Further, he has no information about the framework topology. In our issue, there is no central energy to instate customers. Each of them can be instated self-governing using PKI. [2]

In this paper, a component approved assembling key declaration tradition is shown using mixing for improvised frameworks. In Join figuring, the amount of transmitted messages does not augment with the amount of all social event people, which makes the tradition more practical. The tradition is provably secure. Its security is shown under Decisional Bilinear Diffie-Hellman supposition. The tradition in like manner gives various distinctive securities property [3]

In this paper, gathering key simultaneousness with center affirmation arrangement has been proposed. It's a changed structure which unites the segments and advantages of both Flexible Robust Group Key Agreement and moreover Efficient Authentication Protocol for Virtual Subnet tradition. The central purpose of inclination of proposed arrangement is that it gets rid of the need to send the distinctive parameters for confirmation and furthermore assembling key responsibility [3]. This paper addresses an entrancing security issue in remote uniquely designated framework: the dynamic Group key Agreement key establishment. For secure get-together correspondence in Ad hoc framework, a social event key shared by all part. In this paper maker proposed a novel secure flexible and capable Region-based assembling key comprehension tradition for Ad hoc framework [6].

A Group Key Agreement (GKA) tradition is an instrument to set up a cryptographic key for a social affair of individuals in light of each one's dedication, over an open framework. The key, thusly surmised, can be used to set up an ensured channel between the individuals. In this paper, Author show a direct, secure and profitable GKA tradition fitting to component improvised frameworks. We also display outcomes of our utilization of the tradition in a model application [7].

This paper displays a successful contributory social event key comprehension tradition for secure correspondence between the lightweight little devices in subjective radio compact exceptionally named frameworks. A Ternary tree based Group ECDH.2 (TGECDH.2) tradition that uses a bunch rekeying figuring in the midst of enlistment change is proposed in this paper. This ternary tree is a balanced key tree in which appropriate insertion point is decided for the joining people in the midst of rekeying operation. TGECDH.2 joins the computational viability of ECDH tradition and [8].

III. PROPOSED APPROACH

In proposed framework we execute 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 actualize a solid symmetric encryption for enhancing record security in the framework. The proposed work is wanted to be completed in the accompanying way:

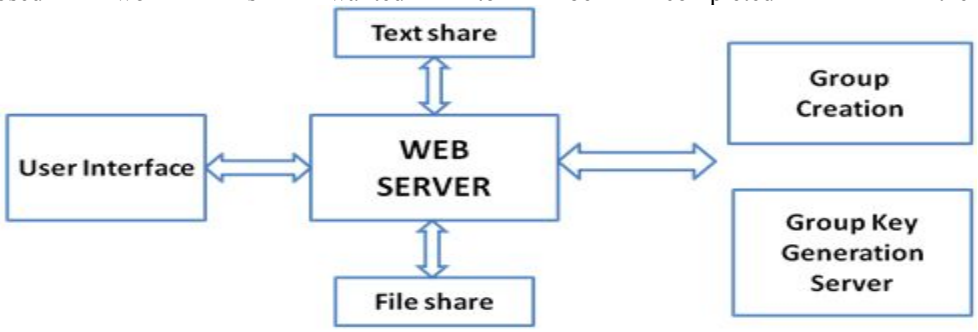
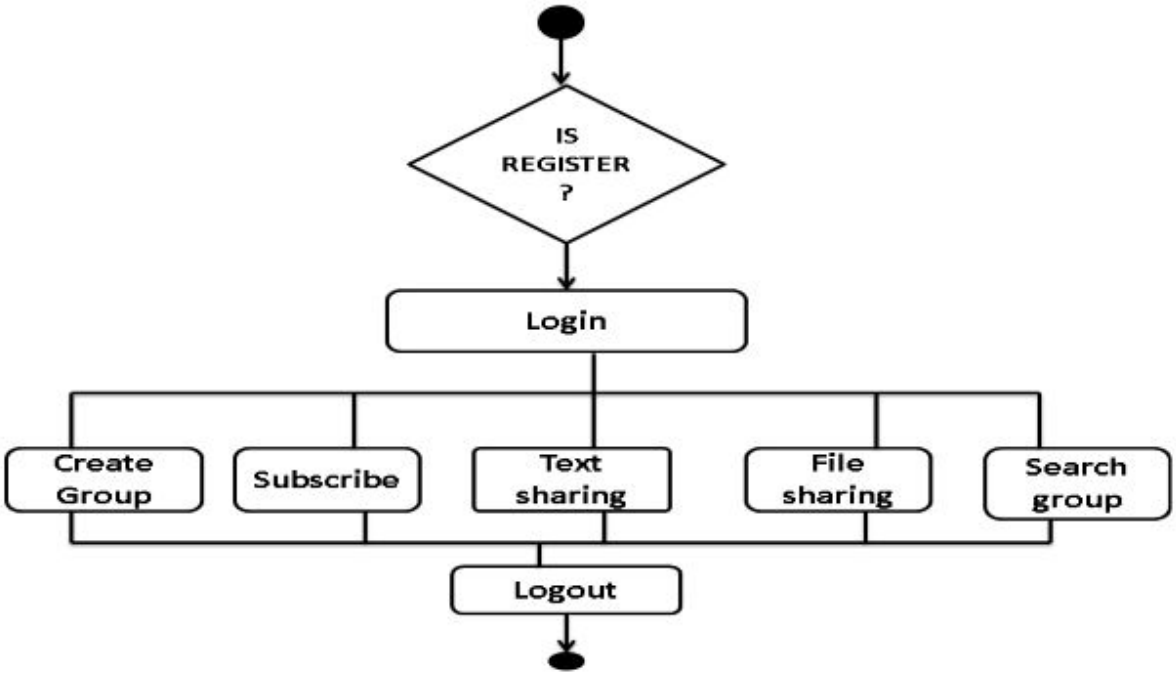


Fig: System Architecture of group key agreement

ISSN 2348 – 8034
Impact Factor-4.022

FLOWCHART:



IV. METHODOLOGY

MODULES

- **Group based information sharing web Application**

These days, bunch situated applications are extremely well known and can be isolated into one-to-numerous, few-to-numerous, and any-to-any applications. Among these, we are keen on any to any applications. Generally this sort of use, for instance, video meeting, is communitarian and such cooperative applications needs peer bunch fundamental. This gathering additionally requires rich correspondence semantics and more tightly control of individuals and put accentuation on unwavering quality and security.

We will create online application that will give bunch visit and document sharing administrations.

- **Data Encryption**

The information to be offer will be scrambled utilizing AES Algorithm .the key will be produced utilizing key era server.

- **File Sharing**

Information to be offer will be in type of content or sight and sound record.

- **Rekeying**

Key administration is a building obstruct for all other cryptographic and secure applications.

ISSN 2348 – 8034
Impact Factor-4.022

At whatever point a client joins or leaves a gathering the multicast key server will produces a key and give to all client of separate gathering.

- **Majority based voting plan usage**

At whatever point a client subscribe to some gathering the lion's share based voting convention which will choose whether to favor or rejected client asked for taking into account larger part assemble.

Group Key Agreement Algorithm

1. Each gathering part contributes its (equivalent) offer to the gathering key, which is processed as an element of all shares of current gathering individuals.

2. This offer is mystery (private to every gathering part) and is never uncovered.

3. As the gathering develops, new individuals' shares are figured into the gathering key however old individuals' shares stay unaltered.

4. As the gathering shrivels, withdrawing individuals' shares are expelled from the new key and no less than one remaining part changes its offer

5. Current gathering individuals' shares are demonstrated as leaf hubs in a parallel tree

6. Each connection (edge) in the tree is named f (k) where k is the estimation of the hub underneath the connection

7. Each non-leaf hub is named f (kl kr) where kl and kr are the names of the left and right youngster hub, individually

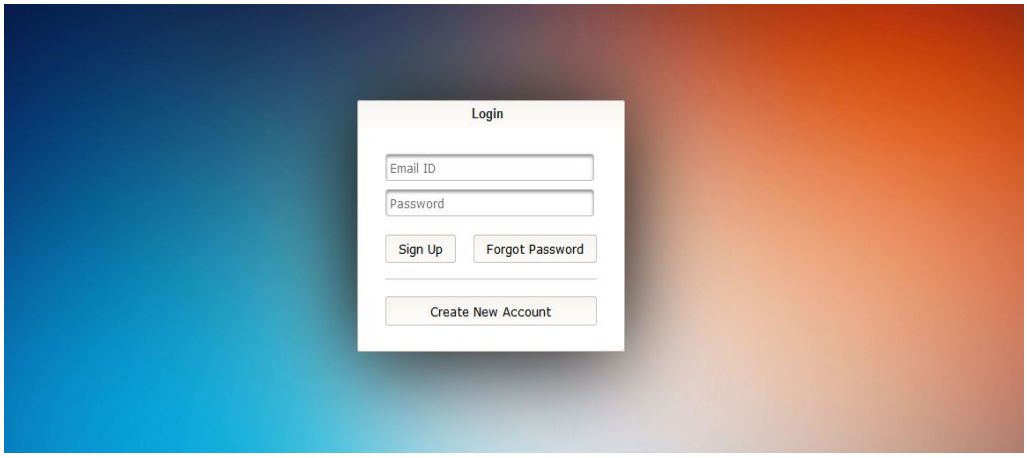
8. The specific capacity f () utilized as a part of our conventions is secluded exponentiation in prime-request bunches, i.e., f (k) = k (mod p)

9. Computing the named estimation of a non-leaf hub requires the information of the estimation of one of the two youngster hubs and the estimation of the other episode join (i.e., join esteem radiating from the other kid hub).

10. All convention messages are marked by the sender. (We utilize AES for this reason).

V. DESIGN WORK

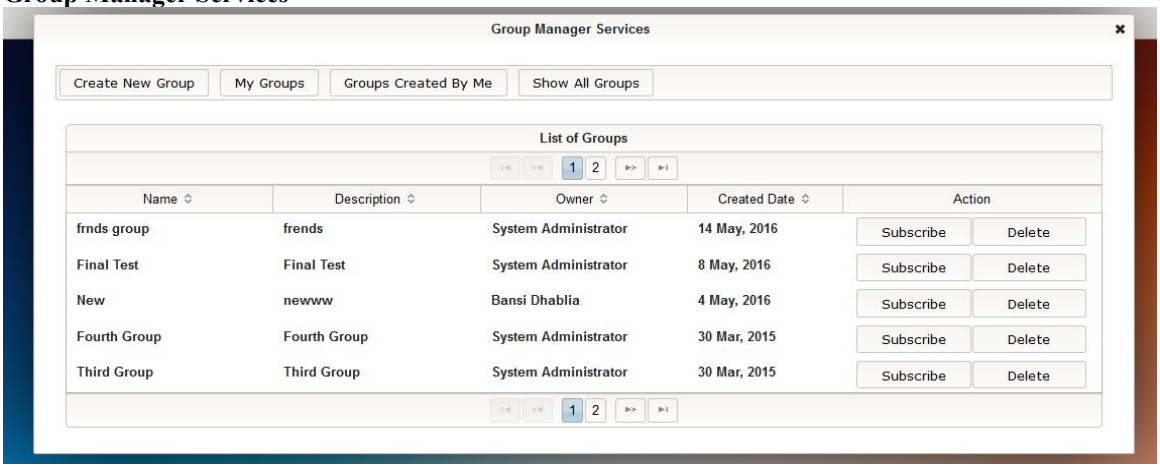
- **Login Module**



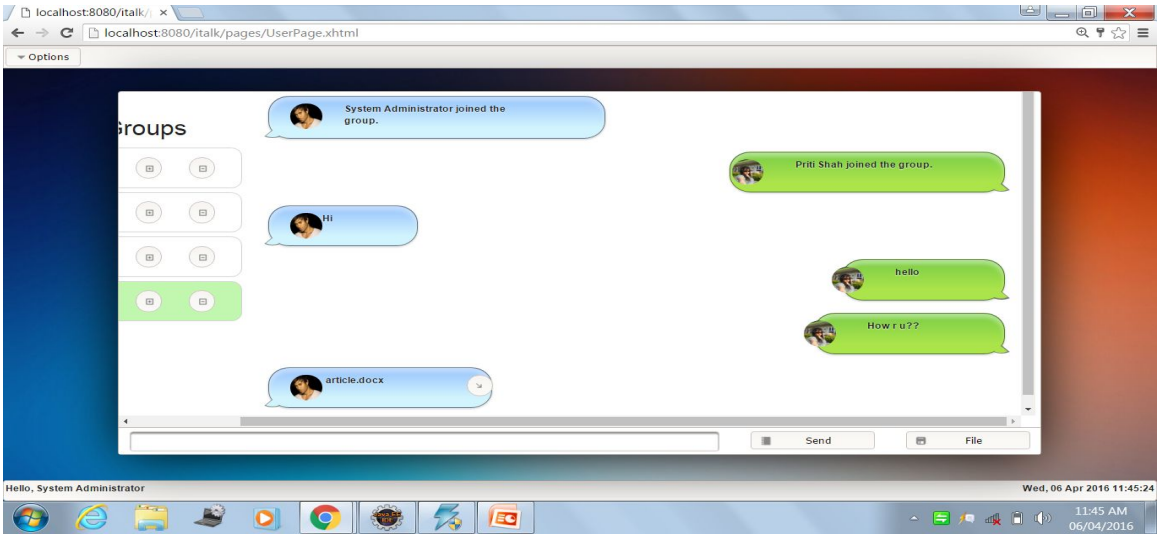
- **Data Encryption**

ISSN 2348 – 8034
Impact Factor-4.022

- **Group Manager Services**



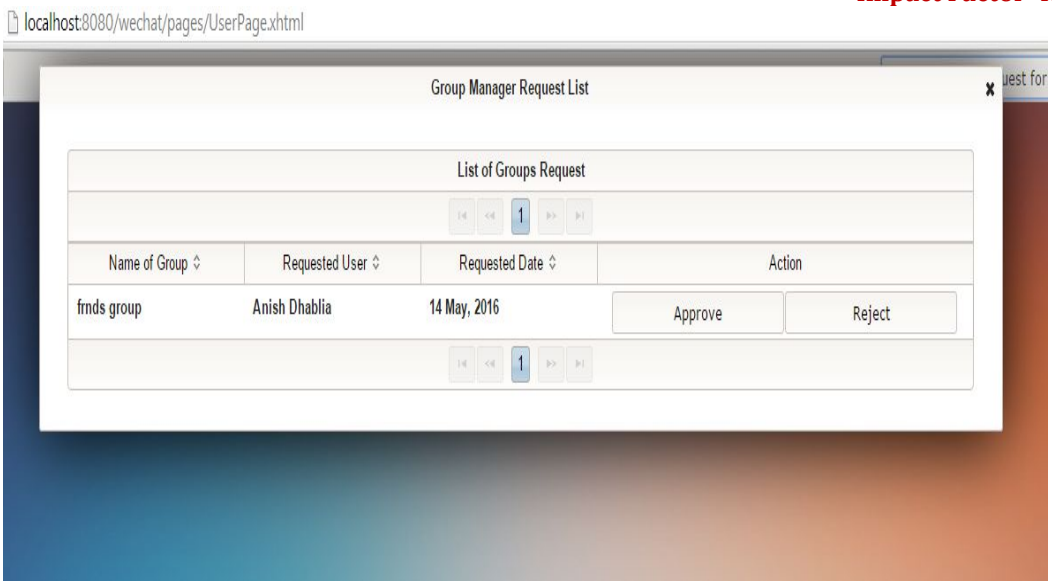
- **File Sharing**



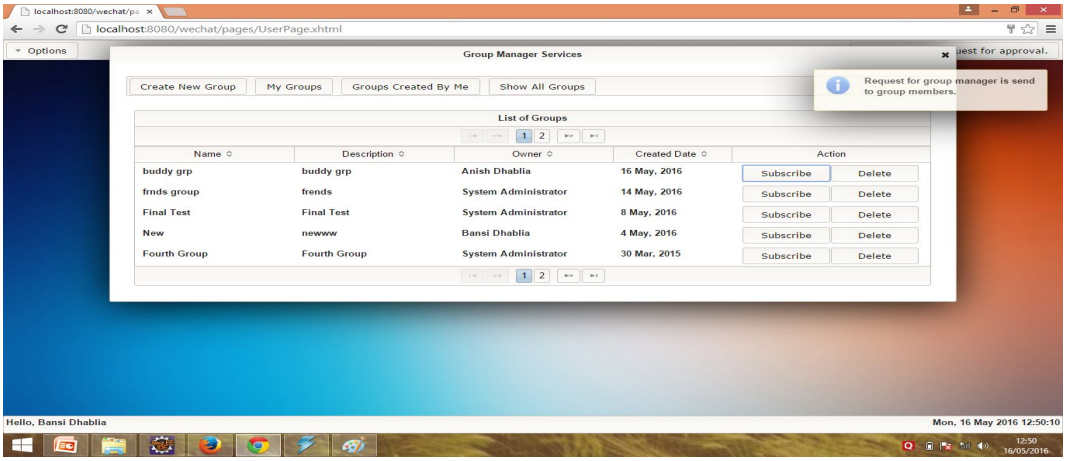
- **REKEYING**

Group Manager Request service

ISSN 2348 – 8034
Impact Factor-4.022



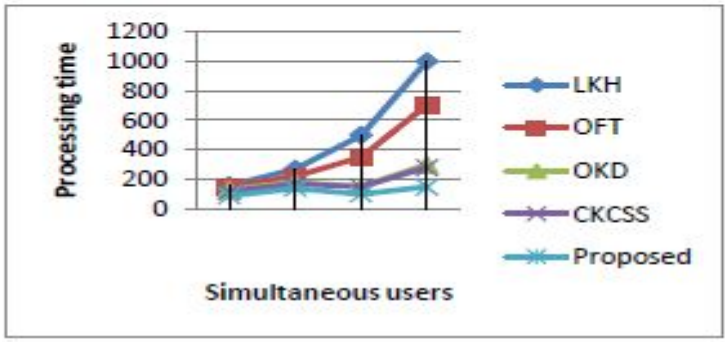
- **Majority Based Voting Scheme**



VI. RESULTS AND DISCUSSION

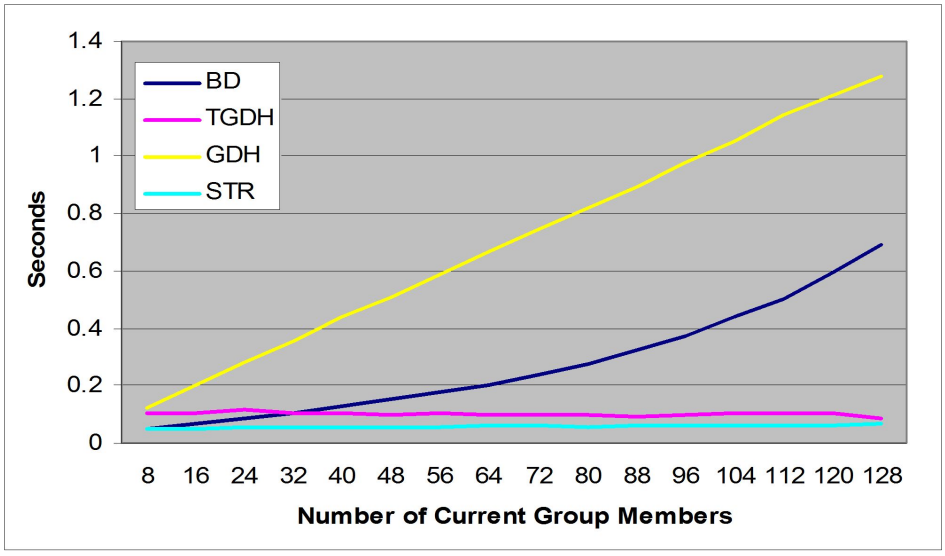
Comparisons:

We introduced a correlation that demonstrates the unpredictability of the gathering era and the preparing time of the process.Table1.The examinations of key era in concurrent join or leave operations are demonstrated as follows.



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)

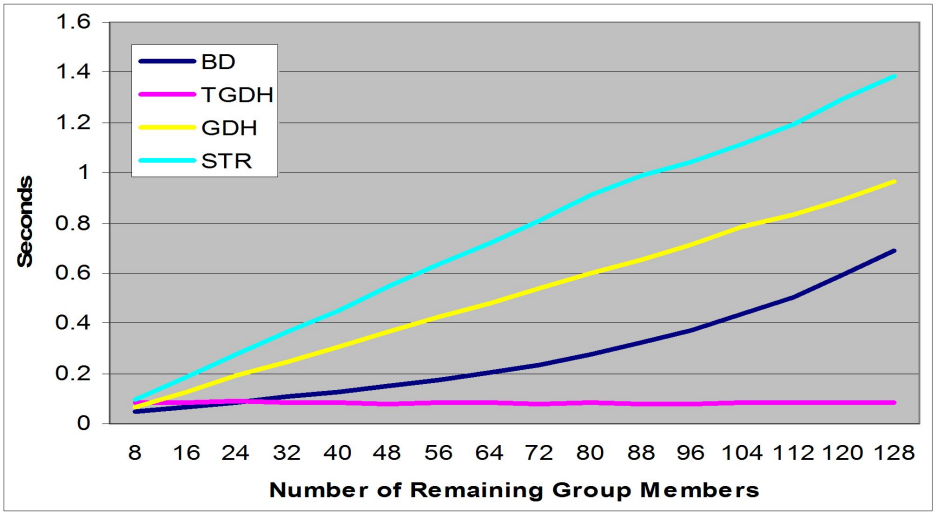
- Computational Cost (Join and Leave)



The above graph shows a x-axis: # members before join

- TGDH, STR: almost 0.1 sec

- GDH worst
- TGDH: Joining node is near to root due to random tree



The above graph shows

- x-axis: # members after leave
- TGDH best
- STR worst

VII. CONCLUSION AND FUTURE ENHANCEMENT

We considered a get-together key comprehension issue, where a customer is only aware of his neighbors while the system graph is subjective. Besides, are instated absolutely self-ruling of each other. A social event key affirmation in this setting is greatly reasonable for applications, for instance, casual groups. We audit particular plans proposed in this space and contemplated that much work is ought to have been be done in this understanding traditions. We encourage propose a voting based tradition arrangement for better assurance and security in social occasion based circumstances.

In future one can either propose, enhancing quick basic leadership utilizing timing based convention. Furthermore, giving individual talk rooms to clients. What's more, the task can likewise be reached out by executing some system in versatile application stages.

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.