Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 10, October-2017

Providing Security to Group Based Communication System with Multicast Key Agreement

Priyanka P. Ghotekar[1], Ketki. R. Ingole[2]

[1]*ME Student, Department of Computer Science and Engineering, SIPNA College of Engineering and Technology, Amravati, Maharashtra, India*

[2]*Associate Professor, Department of Computer Science and Engineering, SIPNA College of Engineering and Technology, Amravati, Maharashtra, India*

Abstract —In this work, an investigation of gathering key understanding issue hosts performed 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 diagram, 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. Here actualize the current framework with additional time productive way and give a multicast key age server. Here is a substitution of the Diffie Hellman key trade convention by another multicast key trade convention that can work with balanced and one to numerous usefulness. Additionally tend to actualize a solid symmetric encryption for enhancing document security in the framework. Here give a greater part based client decision voting calculation for legitimate key administration in assemble condition.

Keywords- Group Key Agreement, Diffie-Hellman, Authentication, Multicast Key Exchange Protocol, Encryption, Majority Based Voting Scheme

I. INTRODUCTION

In scattered structure, here gathering key declaration custom acknowledges an essential part. These are wanted to give a social gathering of clients with a run of the mill question key to such an extent that the clients can safely chat with each other over an open system. Get-together key appreciation suggests different social events need to influence an average to conundrum key to be utilized to trade data safely. In this work consider the social event key concurrence with a confident framework chart, where every client is just mindful of his neighbors and has no data about the region of different clients. Further, he has no data about the system topology. In our issue, there is no central imperativeness to instate customers. Each of them can be instated uninhibitedly using PKI. A get-together key affirmation for this setting is remarkably reasonable for applications, for case, a relational alliance. Under our setting, here, make two advantageous without moving secure traditions. here is a way indicate bring down breaking points on the round Complexity which shows that our traditions are round equipped. In incredibly chose system, the clients are normally flexible. The social gathering part isn't known early and the clients may join and leave the party an awesome piece of the time. In such conditions, segment gathering key perception conventions are required. Such orchestrates must guarantee that the get-together session key updates after social gathering part changing such cap ensuing session keys are shielded from the leaving individuals and past session keys are shielded from the joining individuals. There are largely that vastly different part assembling key perception conventions. Client security surmises that any leaving part from a social event can't make new gathering and joining part into a party can't find ahead of time utilized amassing key.

Confirmation is the way toward deciding if somebody or something is, truth be told, who or what it is pronounced to be. In private and open PC systems (counting the Internet), confirmation is normally done using logon passwords. Learning of the secret key is accepted to ensure that the client is real. Every client enlists at first (or is enrolled by another person), utilizing an appointed or self-pronounced secret word. Secure and solid gathering correspondence is a dynamic region of research. Its fame is caused by the developing significance of gathering focused and community applications.

The focal research challenge is secure and productive gathering key administration. While brought together strategies are regularly suitable for enter dissemination in vast multicast-style gatherings, numerous community assemble settings require circulated key understanding systems. Numerous applications in Dynamic Peer Group are getting to be noticeably expanding famous these days. There is a requirement for security administrations to give bunch arranged correspondence protection and information trustworthiness. To give this type of gathering correspondence protection, it is vital that individuals from the gathering can set up a typical mystery key for scrambling bunch correspondence information. A protected dispersed gathering key understanding and confirmation convention is required to deal with this issue. Incorporated conventions depend on a unified key server to proficiently appropriate the gathering key.

II. LITERATURE REVIEW

Zongyu Song, PengfeiCai, Jie Yang, proposed a part acknowledged collecting key announcement convention is indicated utilizing blending for imprompt systems. The custom is provably secure. Its security is shown under Decisional Bilinear Diffie-Hellman supposition. The custom in like way gives different various securities property. Anurag Singh Tomar, Gaurav Kumar Tak, Manmohan Sharma, proposed collecting key concurrence with focus point attestation course of action. It's a changed from which joins the parts and preferences of both Flexible Robust Group Key Agreement and besides Efficient Authentication Protocol for Virtual Subnet convention .

K. kumar, j. Nafeesa Begum , Dr V. Sumathy, proposed addresses an intriguing security issue in remote particularly chose system: the dynamic Group key Agreement key foundation. For secure get-together correspondence in Adhoc structure, a social affair key shared by all part. A mobile ad hoc network is a collection of autonomous nodes that communicate with each other. Mobile nodes come together to form an ad hoc group for secure communication purpose. A key distribution system requires a trusted third party that acts as a mediator between nodes of the network. Ad-hoc networks characteristically do not have a trusted authority. Group Key Agreement means that multiple parties want to create a common secret key to be used to exchange information securely. Furthermore, group key agreement also needs to address the security issue related to membership changes due to node mobility. The membership change requires frequent changes of group key. This can be done either periodically or updating every membership changes. The changed group key ensures backward and forward secrecy. With frequent changes in group memberships, the recent researches began to pay more attention on the efficiency of group key update. Recently, collaborative and group –oriented applicative situations like battlefield, conference room or rescuer area in mobile ad hoc networks have been a current research area. Group key agreement is a building block in secure group communication in ad hoc networks. However, group key agreement for large and dynamic groups in ad hoc networks is a difficult problem because of the requirements of scalability and security under constraints of node available resources and node mobility.

III. METHODOLOGY

Modules

A. Registration Module :
Here, new user can register itself.

B. Group Chat :
Group chat allows the group members to talk together in a respective group.

C. Data Encryption :
The data to be share is encrypted using AES Algorithm .The key is be generated using key generation server.

D. File Sharing :
Data to be share are in the form of text or multimedia file.

E. 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 generates a key and provide to all user of respective group.

F. Majority based voting scheme **:**
Whenever a user subscribe to some group the majority based voting protocol which decides whether to approve or reject the user requested, based on group majority.

System Implementation

This is the customer module. This is Home page here we can login the new client for enrollment. In the event that the client as of now enroll then login from a similar page. In that underneath page, here to fill the points of interest of the specific client.

Fig 1. New Registration page

In that below page, after user get registered. He/she can login to their account with this page.

Fig 2. Login page

In this page we can see that, there is a group manager service, in which user can create new group. Again user can see all the services of group communication.

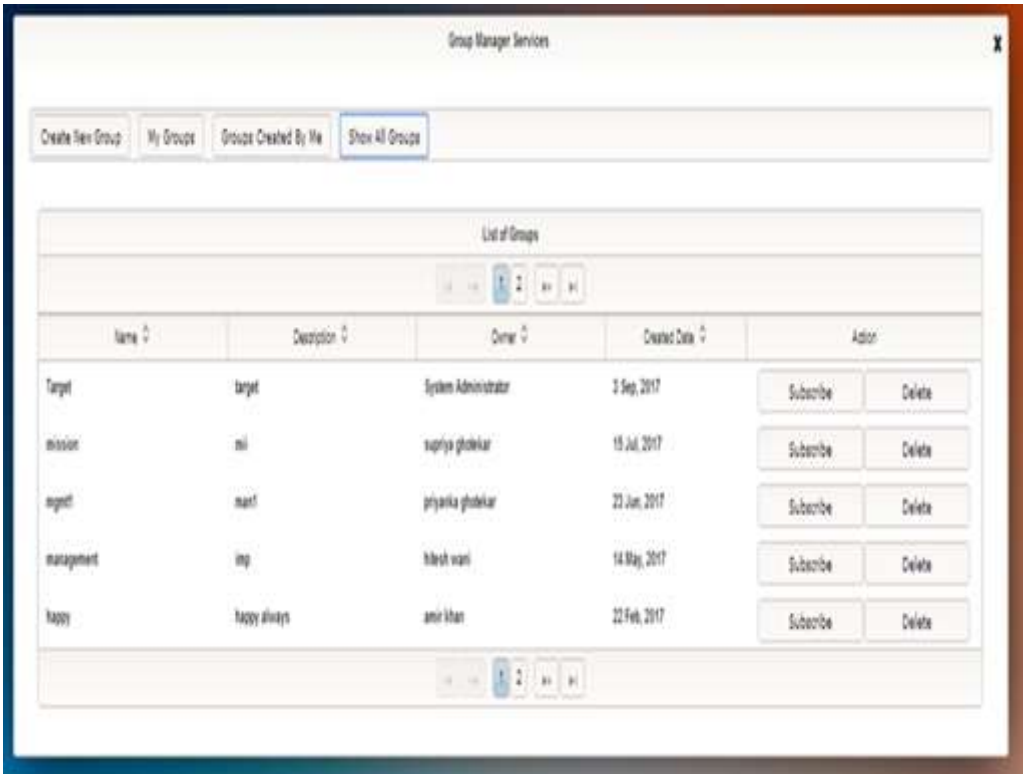

Fig 3. Group Manager Services

Here, this is a new group creation page, user can create new group and can add the number of members according to his/her choice.

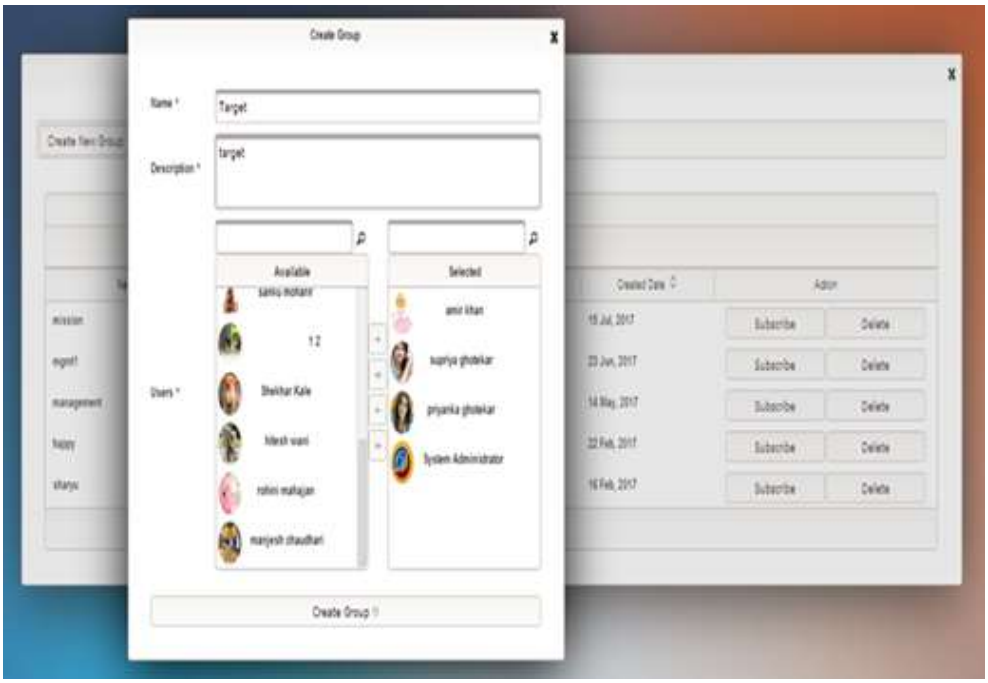

Fig 4. New Group Creation

Once the group get created, the members of group can chat together. Share the files together in secure way.

Fig 5. Group Chat

Here, this page show that whenever the new member get join the group then key for that particular group get changed.

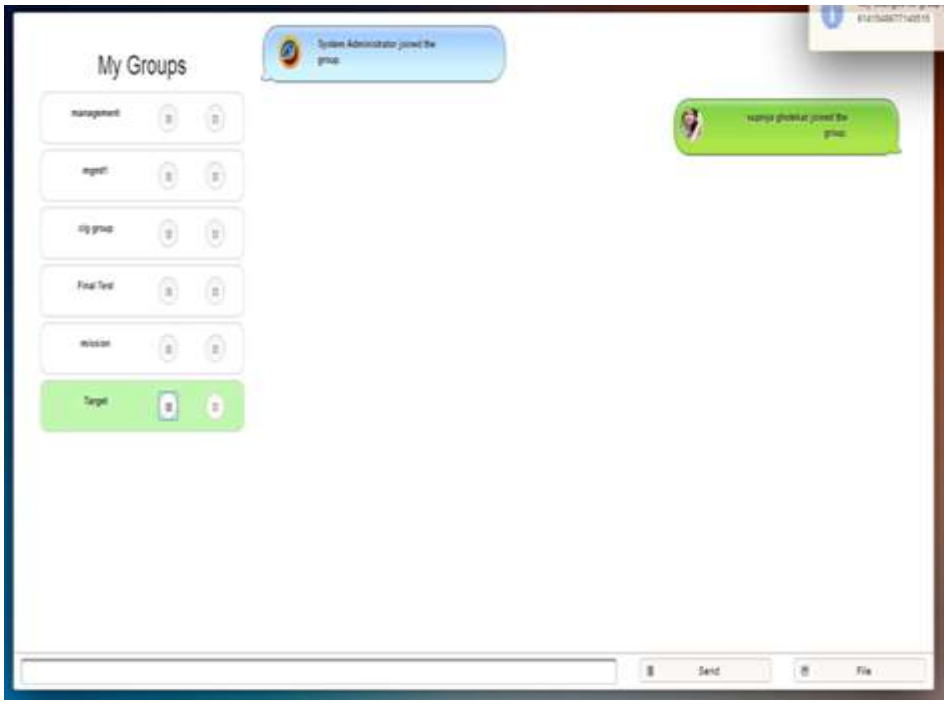

Fig 6. Member Join

When chat is going on, at that time if any of member left the group then the remaining members get that notification.

Fig 7. Member Leave

In this page, we can see that the image file is zip and it is only unzip by the authenticated user.

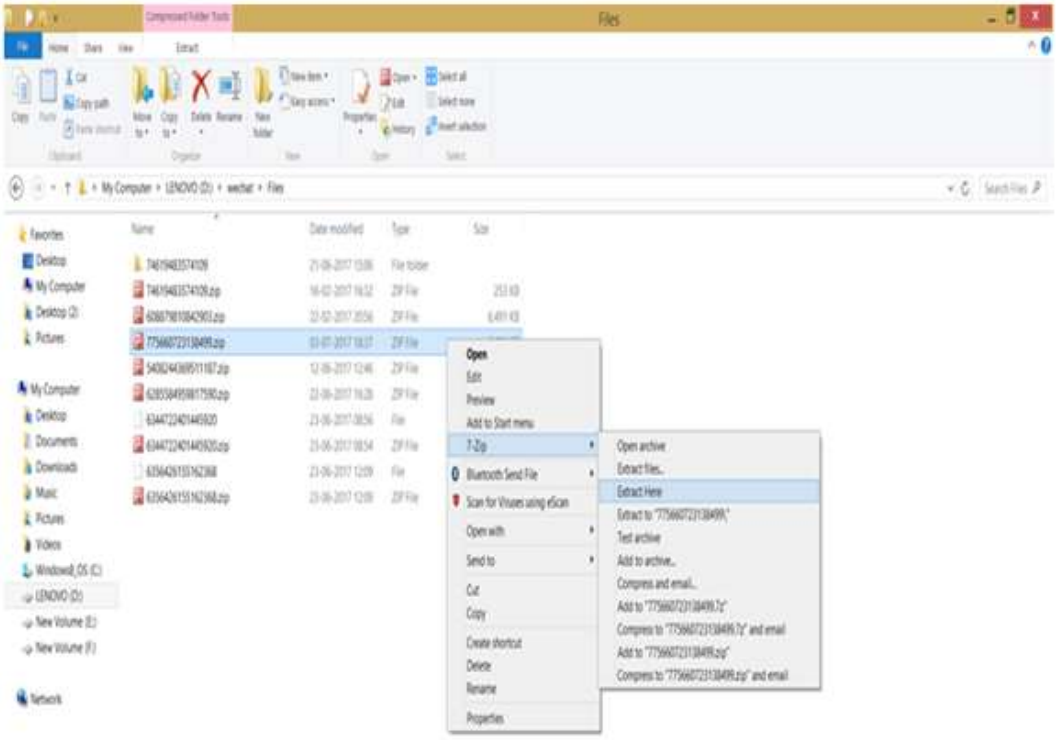

Fig 8. File Unzipping

In below figures, we can see that the image file is decrypted by the authenticated user to see the encrypted file.

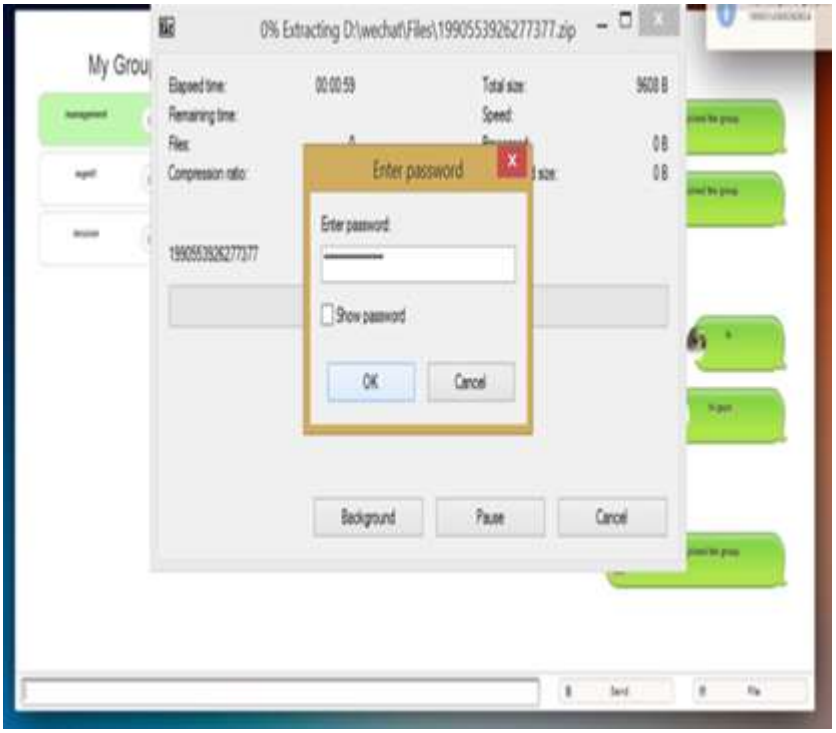

Fig 9(a). File Decryption by authenticated user

Fig 9(b). File Decryption by authenticated user

This page shows that the user is requesting to subscribe for new group and this request is goes to all the members of that group for approval. Majority is responsible to approval for the same.

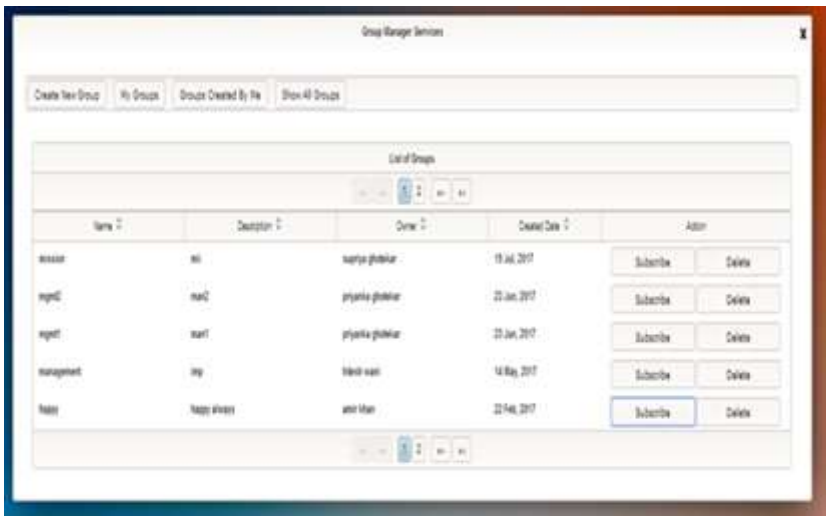

Fig 10. User is requesting to subscribe new group

This page shows that the Group member got the request from user for that particular group, and that group member have the rights to approve or reject.

Fig 11. List of group request

This page shows that the group owner is deleting the group and there is no need take the permission of all other members of the group for the same.

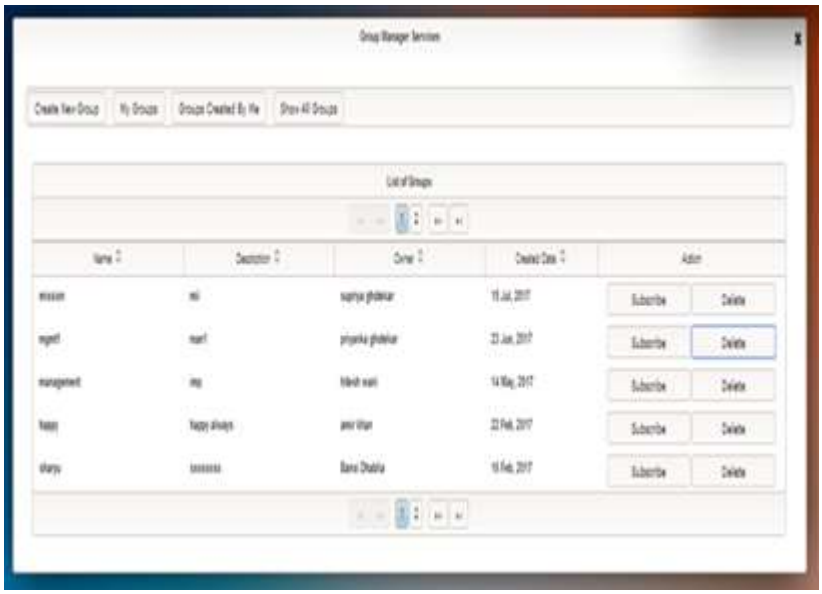

Fig 12. Group owner is deleting the group

IV. EXPERIMENTAL RESULT

This is a framework which is executed for gather correspondence, here all the gathering individuals share mystery key for information encryption while conveying together. Again the multicast key understanding convention is actualized, and the greater security is given by changing gathering key at whatever point the new part gets joined and left. Additionally the cloud auto demolish include is actualized to clear the information at whatever point the individuals get logout.

Analysis
Here, some properties are considered and those properties are implemented.

Table 1. Analysis table

Considerations	Description
Data Security	AES-256 bit key and Random key generation for users
Key Security	Random key generation for every group
Key Agreement	Key changes on Join/Leave
Zipping	File compression is provided
Members contribution	Majority based voting algorithm

Comparisons:
Here is a comparison that shows some differences between the Existing systems and The Proposed System.

Table 2. Comparison between Existing and Proposed system

Existing System	Proposed System
Unicasting, Broadcasting	Multicasting
No Data Compression	Data Compression
Admin decision	Majority based voting
Rekeying concept not considered	Random Key generation considered
Used Asymmetric Encryption	Used Symmetric Encryption

Following table shows the unit testing applying on the system.

Table 3: Unit testing test Cases

No.	**TEST CONDITION**	**EXPECTED RESULTS**	**ACTUAL RESULTS**
1.	To Test that zipping of file is properly done.	Properly getting the zip file.	Same as expected.
2.	To Test that Encryption is properly done.	Properly getting the encrypted file.	Same as expected.
3.	To test whether the login is done properly.	Getting negative response for incorrect login name and Password.	Same as expected.
4.	To Test whether the Rekeying is performed properly.	Key should be provided to the group members as join or leave happen.	Same as expected.

V. CONCLUSION & FUTURESCOPE

Gathering based information correspondence frameworks are extremely prevalent now a days and required higher information security. In this work, here is pondering a social event key understanding issue, where a customer is quite recently aware of his neighbors while the framework chart is subjective. Likewise, clients are instated totally free of each other. In proposed framework enhanced the security of existing framework with higher secured encryption and in the meantime brought down the capacity necessity by utilizing zipping. Likewise enhanced key security utilizing irregular key age for client joins or leaves the gathering. Here, additionally proposed a voting based tradition get ready for better assurance and security in social event based circumstances.
In future one can either propose, enhancing quick basic leadership utilizing timing based convention and giving individual visit rooms to clients. What's more, the task can likewise be reached out by executing some technique in versatile application stages.

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, ManmohanSharma "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] Renugadevi ,C. Mala "Ternary Tree Based Group Key Agreement for Cognitive Radio MANETs" in *I.J. Computer Network and Information Security*, 2014, 10, 24-31Published 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. 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.

[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, 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 2014.*

[12] 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.

[13] Yongdae Kim, Adrian Perrig and Gene Tsudik, "Tree-based Group Key Agreement".

[14] Pothala Siva Kiran Kumar, V Sangeeta," A Manageable Method for Multicast Key Management Protocol ",*International Journal of Engineering Trends and Technology (IJETT) – Volume 18 Number2- Dec 2014.*

[15] Firdaus Mah," Group Key Management in Multicast Security".

[16] 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) 3492–3510.

[17] D. Harkins and N. Doraswamy, "A Secure Scalable Multicast Key Management Protocol (MKMP)," Nov. 1997.

[18] H. Harney and C. Muckenhirn, "Group Key Management Protocol (GKMP) Specification," RFC 2093, July 1997.

[19] T. Hardjono, B. Weis The Multicast Group Security Architecture RFC 3740, IETF Network Working Group, March 2004.

[20] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," Proc. Conf. Advances in Cryptology, May 1994.