ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Key Pattern Using Remote Collective Communication

Konduru Sai Sudhakar
M.Tech
Department of Computer Science and Engineering,
Avanthi's St.Theressa Institute of Engineering and Technology,
Garividi, Vizianagaram, A.P 535101, India.

G. Ramadevi
Assistant Professor
Department of Computer Science and Engineering,
Avanthi's St.Theressa Institute of Engineering and Technology,
Garividi, Vizianagaram, A.P 535101, India.

ABSTRACT

The major challenges are to overcome the obstacles of the potentially limited communication from the group to the sender, the unavailability of a fully trusted key generation center, and the dynamics of the sender. Existing key management paradigms cannot deal with these challenges effectively. The problem of efficiently and securely broadcasting to a remote cooperative group occurs in many newly emerging networks. This system facilitates simple yet efficient member deletion/ addition. This new paradigm is a hybrid of traditional broadcast encryption and group key agreement. Even if all the non-intended members collude, they cannot extract any useful information from the transmitted messages. Its strong security against collusion and its implementation friendliness without relying on a fully trusted authority render this protocol a very promising solution to many applications.

Key Words: ***Key Generation, Strong Security, Emerging Networks***

1.1 INTRODUCTION:

In many of the newly emerging networks, there is a need to broadcast to remote cooperative groups using encrypted transmission. Examples can be found in access control in remote group communication arising in wireless mesh networks (WMNs), mobile *adhoc* networks (MANETs), vehicular *adhoc* networks (VANETs), etc [1-5].

In the above group communication scenarios, the common problem is to enable a sender to securely transmit messages to a remote cooperative group. A solution to this problem must meet several constraints. First, the sender is remote and can be dynamic. Second, the transmission may cross various networks including open insecure networks before reaching the intended recipients. Third, the communication from the group members to the sender may be limited. Also, the sender may wish to choose only a subset of the group as the intended recipients [7]. Further, it is hard to resort to a fully trusted third party to secure the communication. In contrast to the above constraints, mitigating features are that the group members are cooperative and the communication among them is local and efficient.

1.2 PURPOSE OF THE SYSTEM:

The main purpose of the system is to provide effective communication from the sender to the group and to provide secure data transmission over the network by using secure key pattern. Even if any non-intended member receives the data he should not extract any useful information from the data he received. Also to avoid complete dependence on the third party key generation centers for generating keys which are used for group communication.

1.3 SCOPE OF THE SYSTEM:

This system is very useful for the group oriented communication where users are working for the same mission. In this system the sender may be remote and can be dynamic. Also the communication may cross various types of networks and there is no need to depend on the fully trusted third party to secure the communication [9-12].

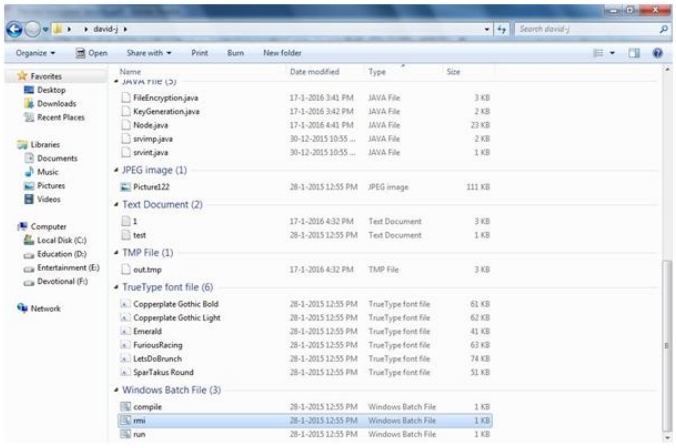
Cite this article as: Konduru Sai Sudhakar & Prof.G. Ramadevi, "Secure Key Pattern Using Remote Collective Communication", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 6 Issue 2, 2019, Page 1-7.

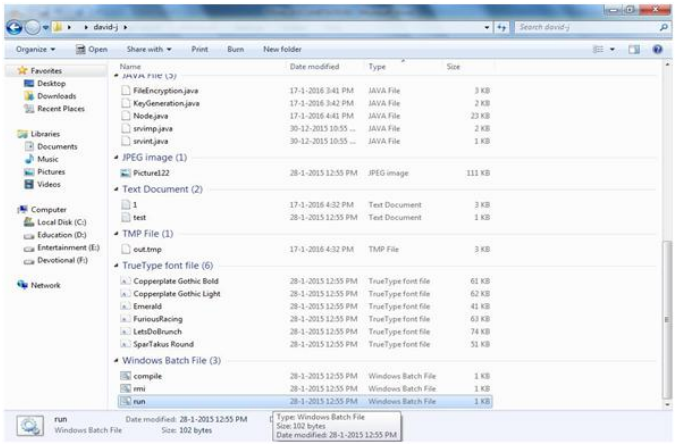
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

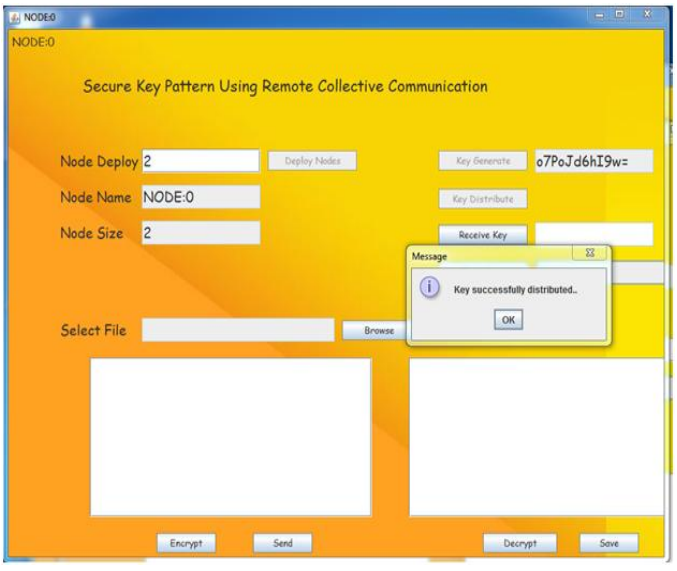
1.4 OBJECTIVE OF THE SYSTEM:

Main objective of the system is to provide effective group communication to the users who are remotely located.

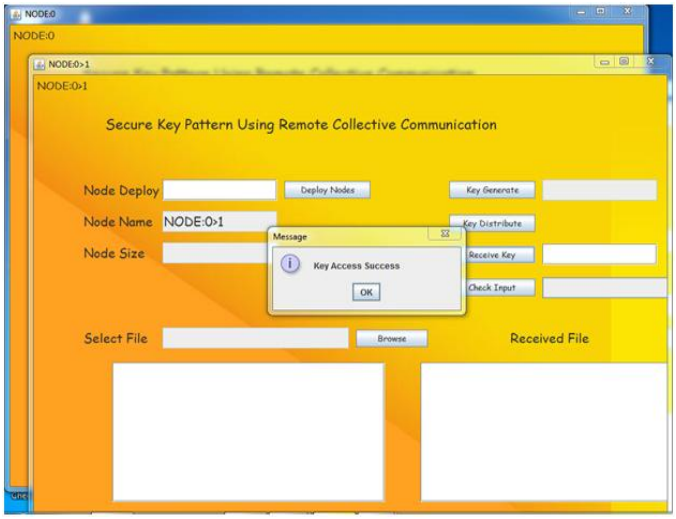
Keeping the data secure by using secure key pattern in such a way that no intended member can read the data.

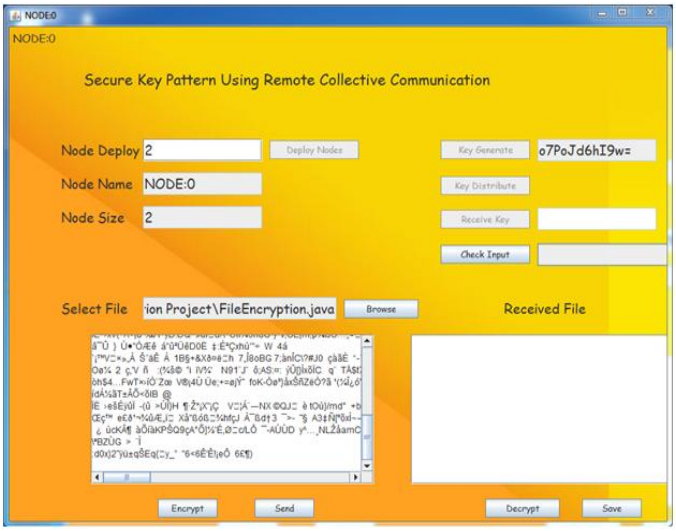


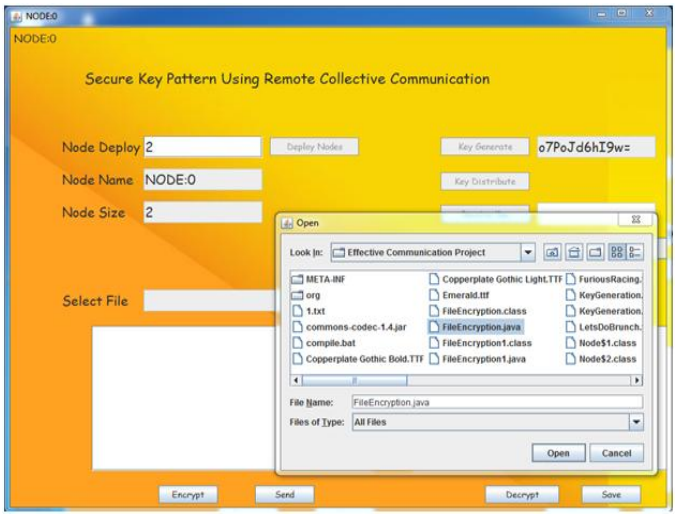


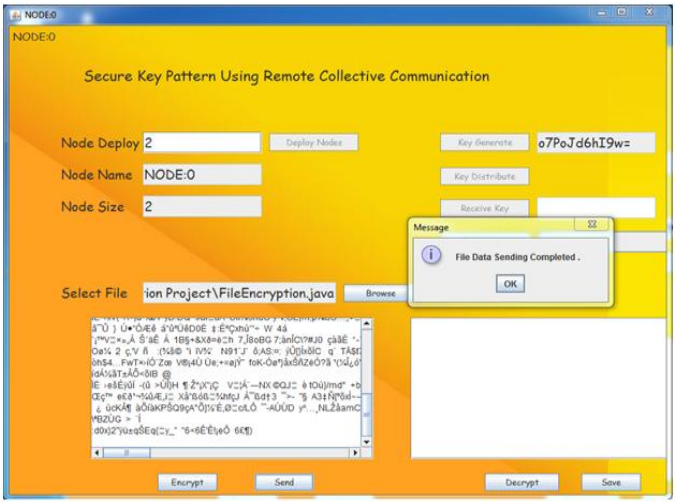


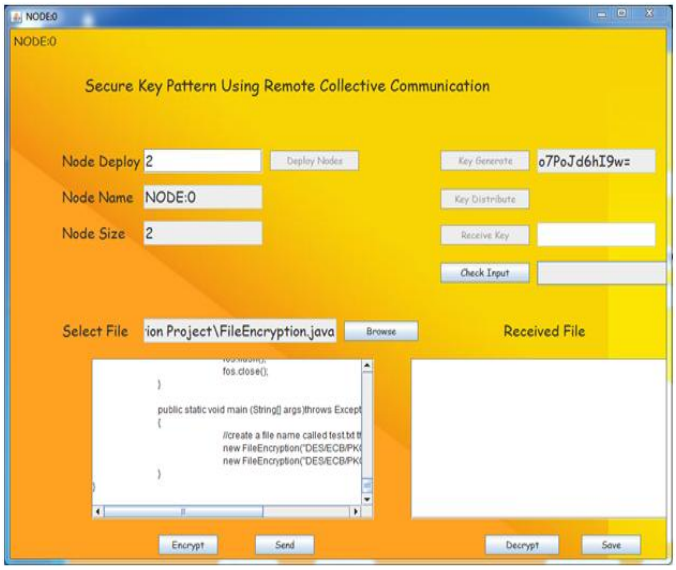
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

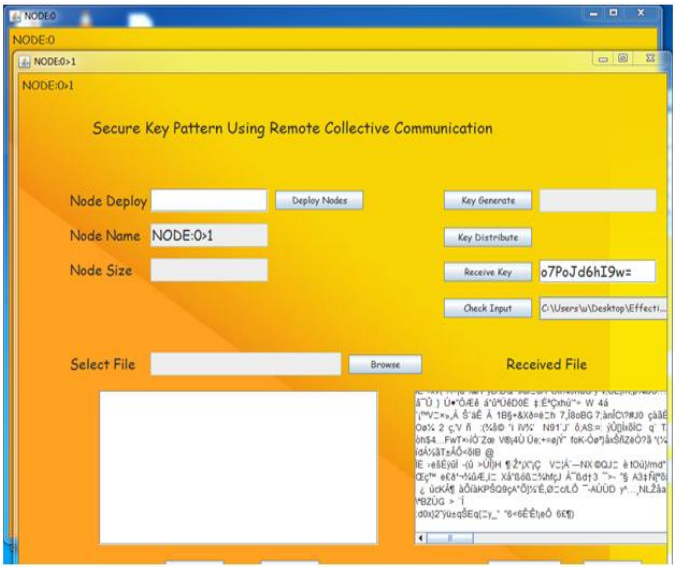




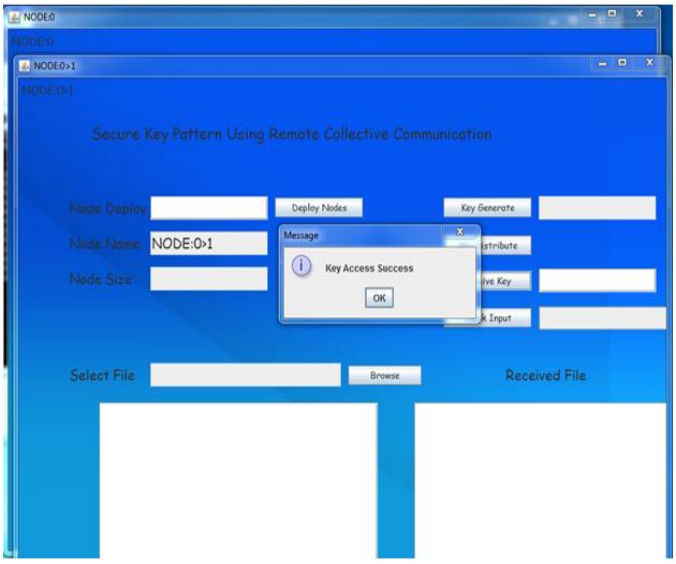


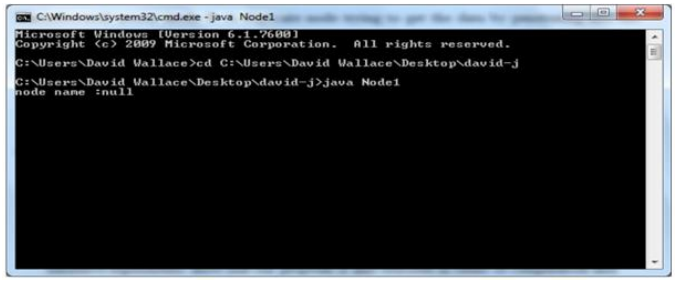


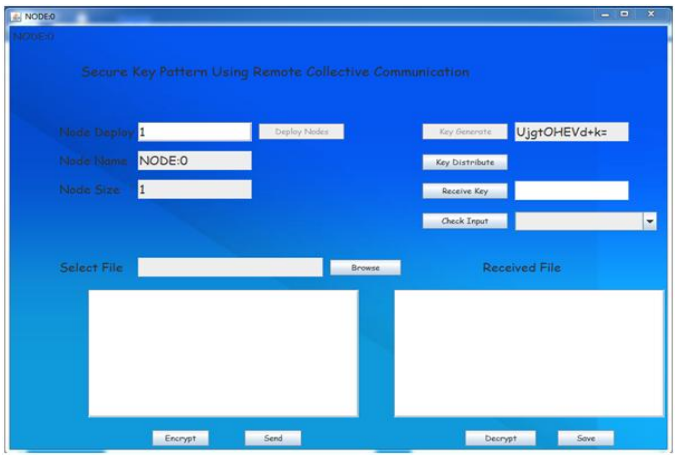


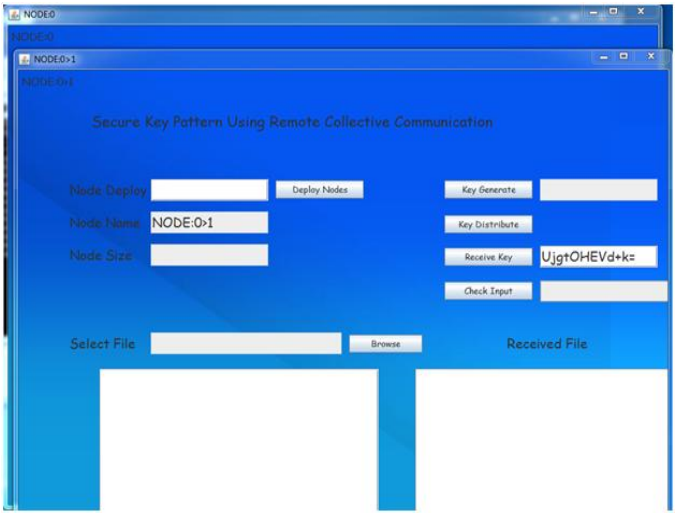


ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

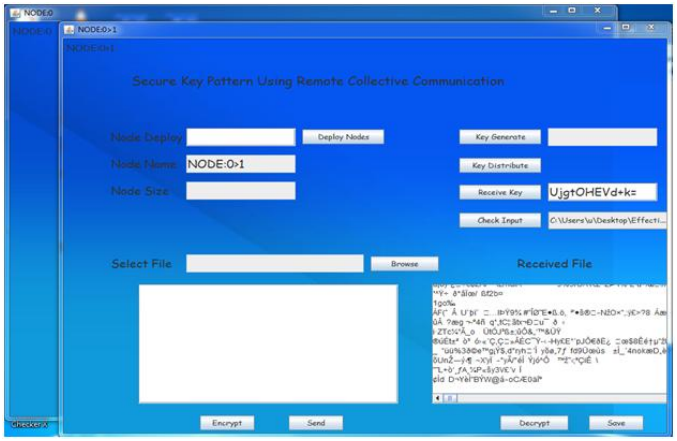








ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



EXISTING SYSTEM:

- Existing key management systems are mainly implemented in two ways referred to as group key agreement and key distribution systems.
- Group key agreement allows a group of users to receive a common secret key via open insecure networks.
- Then any member can encrypt any confidential message with the shared secret key and only the group members can decrypt.
- In a key distribution system, a trusted and centralized key server allocates the secret keys to the users, such that only the privileged users can read the transmitted message.

DISADVANTAGE OF EXISTING SYSTEM:

- The unavailability of a fully trusted key generation center.
- The dynamics of the sender.
- Member addition and deletion is a complex issue.

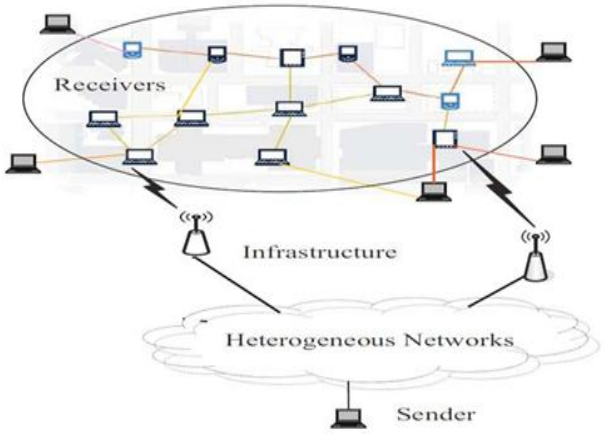
PROPOSED SYSTEM:

The new key management paradigm allows secure and efficient transmissions which is a hybrid of group key agreement and public-key broadcast encryption

ADVANTAGES OF PROPOSED SYSTEM:

- Allows group-oriented communication without relying on a fully trusted secret key generation center.
- New system provides simple and efficient member deletion/ addition.
- The sender may be remote and can be dynamic.

SYSTEM ARCHITECTURE:



Components of the System:

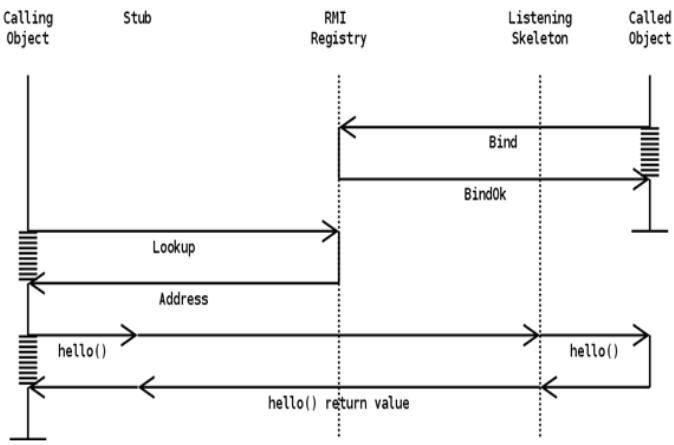
Sender: A person who wants to send the information to other members in the group.

Heterogeneous Networks: Includes different types of networks like Wireless Mesh Networks(WMNs),Mobile Adhoc Networks(MANETs),Vehicular Adhoc Networks(VANETs). Communication may cross all these types of networks.

Infrastructure: Infrastructure includes communication towers, base stations etc.,

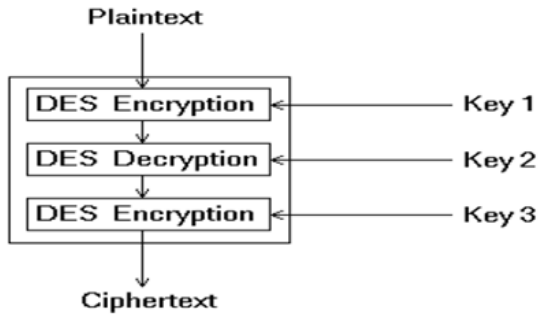
Receivers: The members in the group who are intended to receive the data.

RMI:



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

TDES:



EXAMPLES OF TDES:

The quick brown fox jumped over the lazy dog's back

"The quic"	5468652071756663
"k brown "	6B2062726F776E20
"fox jump"	666F78206A756D70

P1 = "The quic" = 5468652071756663

	Input	Output
DES1 – Encrypt – Key1	5468652071756663	A28E91724C4BBA31
DES2 – Decrypt – Key2	A28E91724C4BBA31	5A2EA7F983A2F53F
DES3 – Encrypt – Key3	5A2EA7F983A2F53F	A826FD8CE53B855F

C1 = A826FD8CE53B855F

6. CONCLUSION AND FUTURE SCOPE

6.1 CONCLUSION

We have proposed a new key management paradigm to enable send-and-leave broadcasts to remote cooperative groups without relying on a fully trusted third party. Our scheme has been proven secure in the standard model. A thorough complexity analysis and extensive experiments show that our proposal is also efficient in terms of computation and communication. These features render our scheme a promising solution to group-oriented communication with access control in various types of ad hoc networks.

6.2 FUTURE SCOPE

This project is having a broad future scope as it can be extended to provide best security for the group oriented communication. We can use advanced encryption and decryption standards for generating the key and also to encrypt and decrypt the data. It can also be implemented in different types of networks without the fear of data theft by the unintended group members or the outsiders. Not only the text files but also the multimedia data like audio, video, images can also be transmitted to the group members using this technology.

REFERENCES:

[1] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multi-hop wireless mesh networks," IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1916–1928, Oct. 2006.

[2] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 2, pp. 203–215, Feb. 2010.

[3] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu, and S. Guizani, "A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study," IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 398–408, Jan. 2009.

[4] Y.-M. Huang, C.-H.Yeh, T.-I.Wang, and H.-C. Chao, "Constructing secure group communication over wireless ad hoc networks based on a virtual subnet model," IEEE Wireless Commun., vol. 14, no. 5, pp. 71–75, Oct. 2007.

[5] Q.Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.

[6] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

[7] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[8] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," Adv. Cryptol., vol. 950, EUROCRYPT'94, LNCS, pp. 275–286, 1995.

[9] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The versakey framework: Versatile group key management," IEEE J. Sel. Areas Commun., vol. 17, no. 9, pp. 1614– 1631, Sep. 1999.

[10] M. Steiner, G. Tsudik, and M. Waidner, "Key agreement in dynamic peer groups," IEEE Trans. Parallel Distrib. Syst., vol. 11, no. 8, pp. 769–780, Aug. 2000.

[11] A. Sherman and D. McGrew, "Key establishment in large dynamic groups using one-way function trees," IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444–458, May 2003.

[12] Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure group communication using robust contributory key agreement," IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 5, pp. 468–480, May 2004.

[13] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," Trans. Inf. Syst. Security, vol. 7, no. 1, pp. 60–96, Feb. 2004.

Author Details

Konduru Sai Sudhakar
M.Tech,
Department of Computer Science and Engineering,
Avanthi's St.Theressa Institute of Engineering and Technology,
Garividi, Vizianagaram, A.P 535101, India.

G. Ramadevi, M.Tech, (Ph.D)
Assistant Professor,
Department of Computer Science and Engineering,
Avanthi's St.Theressa Institute of Engineering and Technology,
Garividi, Vizianagaram, A.P 535101, India.