International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Group Key Agreement with Local Connectivity

[1]PROF. HARISH BARAPATRE, [2]MANSI NAIK, [3]BHAGYASHRI KURLE,

[4]PRATIBHA GHADAGE

[1234]Yadavrao Tasgaonkar Institute Of Engineering And Technology

[1234]Dept. Of Computer Engineering

Abstract - *In computer networks security and secrecy in communication is must. For data transformation, transactions and other various operations need to be Carrie out securely. Group key agreement is an agreement which provides the security in communication of two persons. In social networking it is not possible always to communicate directly with the unknown person. It includes the any third one to communicate through. Group key agreement provides the mechanism in which two users can communicate with each other without intruption or without includeing any third person.In group key agreement mechanism a special key that is called session key is generated. This key is used for the communication.*

1. INTRODUCTION

Group Key agreement is a process of assigning a unique key for communication. In this paper, we studied that on social networks mostly it is not possible to communicate with unknown person directly. Group key agreement provides the mechanism where any two unknown person can communicate directly.

For example on social sites their are groups of people communicate together. But it is not necessary that each and every person in a group well knows each other. Assume their are persons A, B and C. Person A and B are good friends. Person C is a friend of A but B wants to communicate C. So to get the authority to communicate with C , B must have to go through A. Then the communication between them can possible.

But in Group Key Agreement mechanism the directly communication between B and C can possible.

To make this possible we are using the theory of diffie hellman algorithm. Diffie Hellman algorithm provides the key exchange mechanism for communication.

Group key agreement is surly more effective for the social networks. We are using passively secure protocol to construct an actively secure protocol. Which is round efficient.

1.1 EXISTING SYSTEM

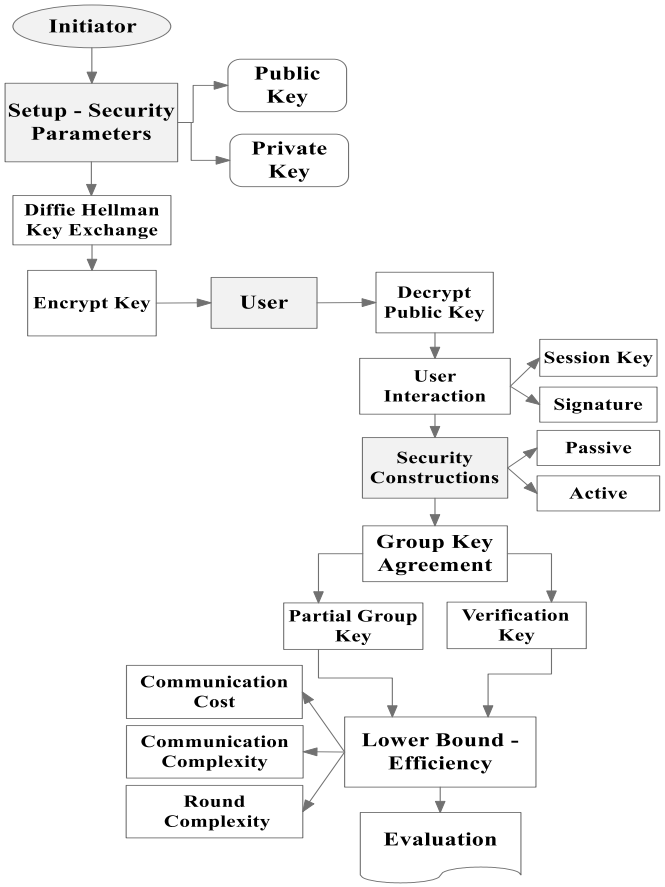
In social networking there are many applications which provide the data connectivity, communication, file transfer, sharing, uploading and many other operations. But sometimes there are problems in communication between two unknown authorities. Most of the systems does not support to the direct connectivity of unknown authorities' for communication or data transfer. However the one person is neighbor of another person who cannot get access with their neighbors directly. So sometimes it makes problem connectivity. So this can be helped with the group key agreement to make it possible.

2. PROPOSED SYSTEM

A **key-agreement protocol** is a protocol where one user is only aware of his neighbors. Two or more parties can agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third parties from forcing a key choice on the agreeing parties. Sender generates key and sends it to receiver. The connection made between is actively secure protocol using passively secure protocol. Protocols that are useful in practice also do not reveal to any eavesdropping party what key has been agreed upon. public-key agreement protocol that meets the above criteria was the Diffie–Hellman key exchange, in which two parties jointly exponentiation a generator with random numbers, in such a way that an eavesdropper cannot feasibly determine what the resultant value used to produce a shared key is. Exponential key exchange in and of itself does not specify any prior agreement or subsequent authentication between the participants. It has thus been described as an anonymous key agreement protocol.

2.1 METHODOLOGY

SYSTEM ARCHITECTURE



3. IMPLEMENTATION

3.1 MODULES:-

1.Repository Creation:

In this module are used to create an user details for who's going to login the local connectivity. So previously they need to create repository.

2.Iniator & User Login

Initiator module used to create a repository as well as create a login id. User login are needed a username and password if its correct then enter into the initiator home else create a repository.

3.Key Generation

Key generation is the process of create a public and private key.After store(save) that keys in the database. If its stored then got a success message or failed or retry to enter the key values.

4.Diffie Hellman

Diffie Hellman algorithm are used in this project.This algorithm are used securely exchange the key from public channel.This algorithm are used to secure the internet services.

5.User Interaction

User interaction module are used to know the current status of the encrypted public key.

6.Security

Security is one of the module in this project.Its is used to ensure the security to unauthorized user's.Public key encryption to private key encryption and private key encryption to public key encryption.

7.Lower Bound

An estimate of a number of operations needed to solve a given problem. Lower bound module is used to display all the details of estimate of problem solving for given problem.

8.Evaluation

Once public and private keys are generated after that encrypt the any one of the key either public or private. After verify the signature of encrypted message. Partial group key are fetched from server then verify it.

4. SOFTWARE DESCRIPTION

The front end of software is developed using Microsoft Visual studio 2008 with .Net and C#. And back end is managed with SQL-Server 2005. Operating system required is from family of Microsoft that means any Microsoft version.

RESULT

Figure 1.Group Key Agreement with Local Connectivity

Figure 2. Communication between users

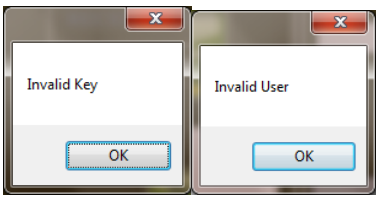


Figure 3. Validating user

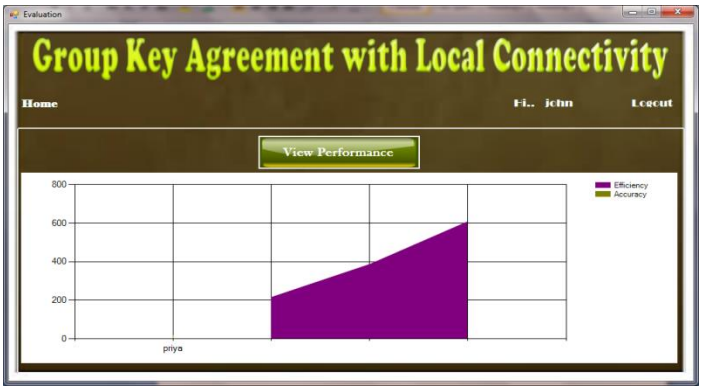


Figure 4. Performance

5. CONCLUSIONS

Here we studied the process of key generation for the security of communication. We generated the actively secured protocols by using the passively secured protocols Key generation is a easy way of communicating secretly on social networks.

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] 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,

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] 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. 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] 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.

[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.