IJCSE International Journal of Computer Sciences and Engineering Open Access

Research/ Review/Survey Paper Volume-5, Issue-8 E-ISSN: 2347-2693

Message And File Transfering Using Key Exchange Protocol Over Secure Network Communication

Reshmi Vijayan[1], Sreedivya R S[2].*

[1] Information & Technology, Govt. Engineering College Barton Hill, Kerala Technical University Trivandrum, India.

[2] Information & Technology, Govt. Engineering College Barton Hill, Kerala Technical University, Trivandrum, India.

e-mail: reshmivijayan30594@gmail.com , rssreedivya@gmail.com

[*]*Corresponding Author: reshmivijayan30594@gmail.com, Tel.: 8281397083, 8078440083*

Available online at: www.ijcseonline.org

Received: 00/…./2017, Revised: 00/…./2017, Accepted: 18/May/2017, Published: 30/Aug/2017

Abstract— Authenticated Key Exchange (AKE) protocol that allows a client and server to communicate each other using generate a session key for suitable and secure communication. The server side will generate a session key after getting approved by the client profile. Here there are single chats and group chats. Here at a time, many users can activate and server also activated for the communication take place. Here there is an encryption and decryption at the time of communication take place using the private key and public key. Finally on the server can also monitoring what all take places on the client side by using remote sensing monitor. Here file transfer also takes place between the user and client with more security. For the communication purpose here it is using intranet so that it can easily find out the IP address of the server and client. The proposed system will be given more importance to the file transferring, remote sensing, protocol used for the key exchange and finally security for the data or file transferring and at a time clients and server will activate and communication takes place and there is a key freshness take place when communication going on after particular time period .The proposed system will be more secure for file transferring over the network communication.

***Keywords*—** Authenticated Key Exchange (AKE) protocol, Encryption and Decryption, IP address , Group chats, File Transferring,CyberMonitorningsystem.

I. INTRODUCTION

The Password-Authenticated Key Exchange protocol allows two parties to establish private and authenticated communication solely based on their shared (low-entropy) password without requiring a Public Key Infrastructure. It provides mutual authentication to the key exchange, a feature that is lacking in the Diffie–Hellman key exchange protocol.

Given that the underlying Schnorr non-interactive zero-knowledge proof is secure, the J-PAKE protocol is proved to satisfy the following properties:

1. Off-line dictionary attack resistance - It does not leak any password verification information to a passive/active attacker.
2. Forward secrecy - It produces session keys that remain secure even when the password is later disclosed.
3. Known-key security - It prevents a disclosed session key from affecting the security of other sessions.
4. On-line dictionary attack resistance - It limits an active attacker to test only one password per protocol execution.

In cryptography, a password-authenticated key agreement method is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password.

An important property is that an eavesdropper or man in the middle cannot obtain enough information to be able to brute force guess a password without further interactions with the parties for each (few) guesses. This means that strong security can be obtained using weak passwords.

1.1 TYPES OF PASSWORD – AUTHENTICATED KEY AGREEMENT:

The Password-authenticated key agreement generally encompasses methods such as:

- Balanced password-authenticated key exchange
- Augmented password-authenticated key exchange
- Password-authenticated key retrieval
- Multi-server methods
- Multi-party methods

In the most stringent password-only security models, there is no requirement for the user of the method to remember any secret or public data other than the password.

In the password-authenticated key exchange (PAKE) is where two or more parties, based only on their knowledge of a password, establish a cryptographic key using an exchange of messages, such that an unauthorized party cannot participate in the method and is constrained as much as possible from brute force guessing the password. Two forms of PAKE are Balanced and Augmented methods.

Password-authenticated key retrieval is a process in which a client obtains a static key in a password-based negotiation with a server that knows data associated with the password, such as the Ford and Kaliski methods. In the most stringent setting, one party uses only a password in conjunction with N servers to retrieve a static key. This is completed in a way that protects the password even if N-1 of the servers are completely compromised.

II. RELATED WORK

In 2005, Fan et al. [1] proposed a two-factor authentication protocol that fails to achieve user anonymity and session key establishment. As it is based on Rabin's public key cryptosystem, Fan et al.'s schemes are less efficient when compared with recent results based on elliptic curve cryptosystems.

In 2004 Das et al. [2] proposed a dynamic ID-based password authentication scheme. Password-based authentication schemes are the most widely used techniques for remote user authentication. Many static ID-based remote user authentication schemes both with and without smart cards have been proposed. Most of the schemes do not allow the users to choose and change their password and maintain a verifier table to verify the validity of the user login.

In 2013 Wang et al.[3] showed that many recently proposed dynamic ID-based Anonymous Two-factor AKE protocols have one or more weaknesses, such as vulnerability against lost-smart-card attack, offline dictionary attack, or lack of forwarding secrecy, anonymity. It is worth noting that, in order to provide user anonymity, almost all dynamic ID-based two-factor authentication protocols need an additional synchronization mechanism to maintain the consistency of the one-time identity between the user and the server.

In 2015, 2016 Chaudhry et al. proposed two schemes [4],[5] that are claimed to achieve anonymity and many other desirable properties, but both of them don't support smart card revocation, and the second scheme [5] does not provide password change mechanism. Besides, we found that the first scheme [4] failed to achieve forward secrecy even though it claimed so because its previous session keys can be recovered if the adversary gets access to the user's password, smart card and protocol transcripts of previous sessions. There are also some other schemes based on biometric techniques or adjusted for the setting of multiple servers [6], [7], which is of independent interest but out of the scope of this paper. Furthermore, the schemes under public key infrastructure may not be suitable for lightweight computation devices. Therefore, it is still an open problem to design a secure and efficient Anonymous Two-Factor AKE scheme without using public keys.

Bresson et al [11] generated a group key for authentication using DH. Katz and Yung [12] proposed first constant round group key protocol based on DH which is secure for standard models. Tzeng [13] proposed a distributed group key based on DH and discrete logarithm (DL). Cheng and Leigh [14] modified the Tzeng's protocol by bilinear pairing. Huang et al [15] used the non-

interactive protocol based on DL to improve the Tzeng's protocol. Secret sharing schemes were introduced by Blakely [16] and Shamir [17] to safeguard cryptographic keys.

III. PROPOSED ARCHITECTURE

The proposed system has 2 methods are taking place they are

(i) Group authentication
(ii) Cyber monitoring system.

In group authentication in one system will act as server and client and another system as the client like that many no of clients are taking place. No: as clients can register and send the request to admin on the server side for the client approval. The admin takes each client profile and after giving approval then send the N password key for group authentication to the client side. After that using the username and password login the authentication page in that there are single chat, group chat, and registered view.

When two or more client of the same group will get the same key. When the communication takes place only with the same group member in the client if they want the private chat with group members then select the particular member of the member of that group. Here encryption and decryption take place automatically when the message sent and received.

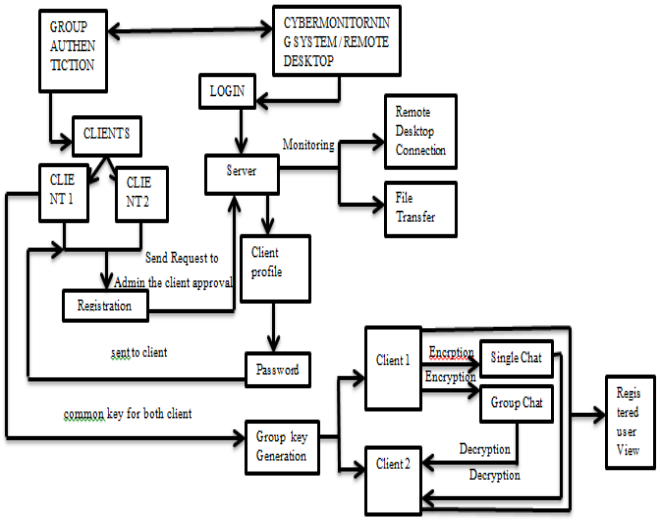

Fig 3.1 The proposed system of the Group authentication and Cyber Monitoring System

In the admin side that is the server if they want to delete the particular member of the particular group admin can delete. In the admin side there is a key generation page is there for monitoring the client side and there it will detect the IP address of the client and it will show what all doing the authentication page from login onwards and it will check the message whether it transferring and reaching properly to the receiver side and it will show what all IP address in what all groups and showing the details of client IP address and desktop name and server IP address. Here the main advantage is when the registered IP address should be matched with server-side then only admin allow the authentication and that much security are provided in the authentication here authentication protocol is the main protocol used for this authentication.

The unauthorized IP address cannot be communicated. If the unauthorized person enters then it will not generate the correct group key for authentication. Here RSA algorithm is used for encryption and decryption at a time both techniques will be executed.

In cyber monitoring system here it will act as remote desktop connection and file transfer. In remote desktop connection in that it will give the IP address of the client than from admin side it can be messaging from one desktop to another desktop that means client desktop then admin can view the client desktop what all information needed that can be accessed from client side then if it wants to log off or restart or close can also be done. In the file transfer system here what all text doc file want to send that can be sent through the registered network in the server to the client desktop while selecting the path by browsing.

Here Group key authentication protocol is used for the secure communication over the network. At a time many clients of the same group can be authenticated each other without logout after particular time the key freshness take place that will provide the security key for the authentication and for encryption and decryption, file transferring and browsing all these processes can take place at a time but in the case of early authentication protocol at a time only either encryption or decryption take place . This proposed system provides more security in the key authentication and files transfer over the network.

IV. SYSTEM IMPLEMENTATION

A. MODULE DESCRIPTION

A.1. GROUP AUTHENTICATION MODULE

In this module first client has to register the client profile and automatically when client register the profile it will show the corresponding IP address of the client where it from it has been registering the profile. After registering the client profile client sent details to admin for the approval of the client profile. In server side, it will automatically come to the notification from the client for the approval. After approving the client profile the server will provide a password for the corresponding client then sent to the client. Then each client uses their username and password for the login. Then the same group members can chat as single chat and group chat each other. When the more than two clients want to chat than for the same group members will get the group key for the communication. In single chat using this group key can chat each other so other members do not see in the same group when one client send the message to another client that message will be encrypted format automatically when it receiving the other side of the client will automatically decrypt the message and receive the message also. For the encryption and decryption here it is used the RSA algorithm. Here authentication protocol is used for encryption, decryption and checking the IP address so that it must have that security to the authenticated key exchange and data transmission. If client registering in group 1 member list then it can chat with group1 members only if it is want to update profile there is an option. In the admin side if the admin wants to delete one of the client profile of one of the group then delete that group. After login the client, he /she can view that who all registered in the same group. In the group chat select the name of the member then we chat in that also it can be encryption and decryption take place. In the server side there is an key generation in that it will display the server and client IP address and who all are login and what all message send , which all IP address in the which all groups when it was logged out all the thing can be view in the server side .when compare with existing system the encryption and decryption of the data time delay will be reduced in the network so that max size of the data can be encrypted and decrypted .And the packet rate also will be varying when the size of the packet increase.

A.2. CYBER MONITORING SYSTEM

In the cyber monitoring system there are two methods are:

1. Remote Desktop Connection
2. File transferring

In the Remote Desktop connection in that server has to give the IP address of the client. Then display the desktop of the client in the server desktop and it can be monitored by the admin. In that there are many options like client details that are getting information about the client desktop and other options like memory information, screenshots, CD drive open and close, installed programs, messaging from one desktop to another desktop, restart, logoff and shut down finally close.

In case of the file transferring here only register IP address only can send the file to the other register IP address in the network. By selecting the path that is for the send file where have to be transferred to either desktop or local disk of any of the drive-by browsings it can select the text file and send to the client desktop. After sending the file then it can close the remote listener.

These two methods and group authentication method are based the authentication key exchange protocol. Based on the IP address of the network it will be performed the process and the unauthorized network cannot perform the communication but dynamic IP address can be registered in the network after that only communication and file transfer take place over the secure network communication.

V . ANALYSIS AND RESULT

A. Performance Comparison

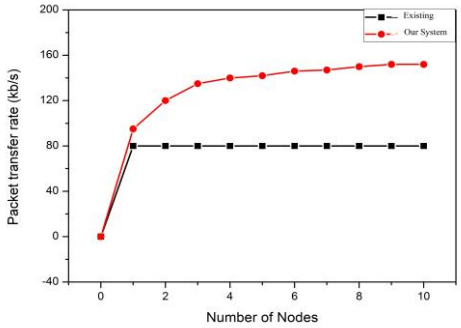

Fig.5.A: Packet Transfer Rate.

In the existing system, the packet transmission rate and group key were stable when the numbers of the node increase also but in the proposed system when the number of the node increase then the packet transmission rate will be increasing and it will be increasing and decreasing according to the number of nodes. If the number of the nodes then it will be varying according to the nodes. So when compared with the existing system then the proposed system has more no of packet transmission rate take place.

B. Encryption and Decryption Time Comparisons of Node Data Security

The node data parameters for data encryption and data decryption time consumption as the improved time for data transmission and the reduced time delay between node network is experiments as shown in Figure 5.1.B(1) and Figure 5.1.B(2).

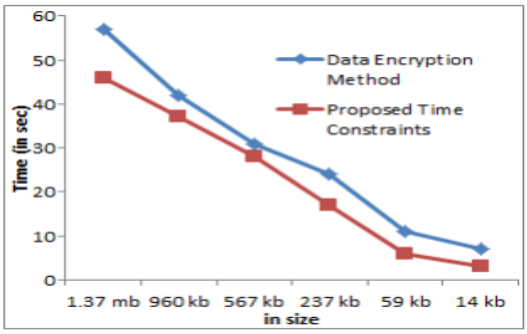

Fig.5.1.B (1): Data Transmission time comparisons with the encryption method

In the proposed system when the size of the encryption data will be high but their time constraint will be less when compared with the existing system time delay between node networks will be high. In the proposed, it will reduce the delay between the nodes of the network.

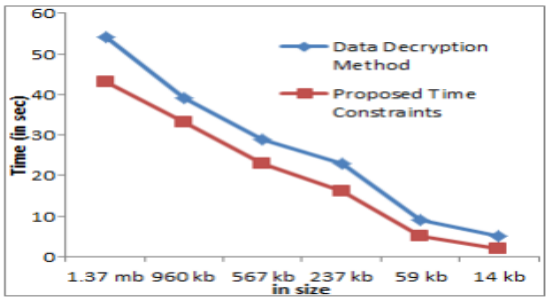

Fig 5.1.B (2): Data Transmission time comparisons with the decryption method.

In the decryption method in the proposed system it will be reduced the delay time between the node of the network whereas comparing with the existing system in the network the delay time will be very high and packet size also high so that much delay occurs in the existing but in the proposed system if the size of the data will be more also then it will be reduced the time delay and decrypting within in the minimum number of time and provide that much security for key also for decrypting the data.

VI . CONCLUSION AND FUTURE WORK

A. CONCLUSION

In this work, the group authentication and widely used for encryption and decryption the data automatically when the communication takes place. Here the key freshness also takes place without disturbing the client's communication automatically key freshness take place after the particular time period and the security of the key size also highly protected for encryption and decryption. The delay of the time constraint also reduced for the maximum size of the data for encryption and decryption when compare with the existing system, the authenticated IP address can only communication take place in the corresponding group members. Here authentication protocol is used because in the early protocol at a time only either encryption or decryption or file transferring take place but in this work, the authenticated key exchange protocol is used for encryption and decryption and file transferring, IP address, browsing take place at the time.

The remote desktop connection / cyber monitoring also take place in that two methods are used file transfer and remote desktop in that also registered IP address can transfer the file from one desktop to another client desktop in that also unauthorized network IP address cannot communicate each other. So that the developed software is tested well with sample data and outputs obtained according to the requirements. The performance of the system is evaluated and found to be efficient. Though it could not be claimed that my project is an ideal project, it will meet the primary security requirements.

B. FUTURE WORK

The Future enhancement is subjected to the user needs and technological growth. The system has been designed and developed flexibly according to the

current requirements of the user. As the security requirements may still increase in the near future, further such development can be attempted.

REFERENCES

[1] C. Fan, Y. Chan and Z. Zhang, "Robust remote authentication scheme with smart cards," Computer. Secure, vol. 24, no. 8, pp. 619- 628, Nov. 2005.

[2] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Trans. Consum. Electron., Vol. 50, no. 2, pp.629-631, 2004.

[3] S. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, and M. K. Khan, "An enhanced privacy preserving remote user authentication scheme with provable security", Security Comm. Networks, 8:3782-3795, 2015.

[4] S. Chaudhry, H. Naqvi, K. Mahmood, H. F. Ahmad, and M. K. Khan, "An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography", Wireless Pers. Communication, DOI10.1007/s11277-016-3745-3, 2016.

[5] S. Chaudhry, "A secure biometric-based multi-server authentication scheme for social multimedia networks", Multimedia Tools Appl.,75:12705-12725, 2016.

[6] A. Irshad, M. Sher, O. Nawaz, S.Chaudhry, I. Khan, and S. Kumari, "A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. scheme", Multimedia Tools Appl., DOI 10.1007/s11042-016-3921-1,2016.

[7] F. Wen, and X. Li, "An improved dynamic ID-Based remote user authentication with key agreement scheme," Computers and Electrical Engineering, 38(2):381-387, 2012

[8] W. Juang, S. Chen, and H. Liaw, "Robust and efficient password-authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., vol. 15 no. 6, pp. 2551- 2556, Jun. 2008

[9] G. Yang, D. S. Wong, H. Wang and X. Deng, "Two-factor mutual authentication based on smart cards and passwords," Journal of Computer and System Sciences, 74(7): 1160-1172, 2008

[10] M. Khan, S.Kim, and K. Alghathbar,"Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications, 34:305-309, 2011.

[11] E.Bresson, O.Chevassut, and D.Pointcheval, "Provably Secure Authenticated Group Diffie- Hellman Key Exchange," ACM Trans. Information and Systems Security, Vol.10, no.3, pp.255- 264, Aug.2007.

[12] J.Katz and M.Yung, "Scalable Protocols for Authenticated Group Key Exchange," J.Cryptology, Vol.20, pp.85-113, 2007.

[13] W.G.Tzeng. "A Secure Fault-Tolerant Conference-Key Agreement Protocol," IEEE Trans.Computer, Vol.51, no.4, pp.373-379,Apr.2002

[14] Johannes A.Buchmann, Introduction to cryptography, second edition, Springer-Verlog NY, LLC, 2005

[15] K.H.Huang, Y.F.Chung,H.H.Lee,F.Lai and T.S.Chen, " A Conference Key Agreement Protocol with Fault-Tolerant Capability", Computer Standard and Interfaces, Vol.31, pp.401-405, Jan 2009.

[16] G.R.Blakley, "Safeguarding Cryptographic Keys", Proc Am. Federation of Information Processing Soc. (AFIPS'79) Nat'l Computer Conf., Vol.48,pp.313-317,1979.

[17] A.Shamir," How to share a Secret ",Comm ACM, Vol.22, no.11,pp.612-613,1979.

