IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol-6, Special Issue-6, July 2018 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 CollegeBarton Hill, Kerala Technical University Trivandrum, India
[2]Information&Technology, Govt. EngineeringCollegeBarton Hill, Kerala Technical University, Trivandrum, India

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

Available online at: www.ijcseonline.org

Abstract— Authenticated Key Exchange (AKE) protocol allows to communicated each other using a generate session key for suitable and secure communication. The server side will generate a session key after giving approval by the client profile. Clients can view other clients of same group who is online at the time. During the message or file transfer both encryption and decryption takes place automatically using RSA algorithm with a symmetric key. Finally the administrator can also monitoring what all take place in the client side by using remote sensing capability. File transfer take place between the user and client with more security. For the communication purpose here it is using intranet so that it can be easily find out the IP address of the server and client. The proposed system will be give more important to the file transferring, remote sensing. The other speciality of the proposed system is key freshness that takes place periodically. 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, Cyber Monitorning system

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.

A. 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

In2005, 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 Dasetal. [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 smartcards 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.

In2013Wang etal.[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 Chaudhry et al.[4] proposed to achieve anonymity and many other desirable properties, but don't support smart card revocation, it found that the 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.

In 2016 Chaudhry et al.[5] proposed a system which does not provide password change mechanism. Besides, There are also some other schemes based on biometric techniques or adjusted for the setting of multiple servers[6], [7], Furthermore, the schemes under public key infrastructure may not be suitable for light weight compu tation 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

- Group authentication
- Cyber monitoring system.

In proposed system the group authentication will be used for the communication among particular group members in an organisation. They can share theconfidential information between each other who are registered in the same group .This use an using asymmetric key with the use of RSA algorithm and authentication key exchange protocol. In group authentication, one of the system will act as both server and client and the rest of the system will be clients. At an instant many number of the clients can be requested for the group authentication. The client has to register the profile with some details. During registration, the client profile page contains an ip address box and client desktop name, both will appear automatically. Ip address is one of the security aid for the group authentication. The group authentication process is done only in intranet. After registering, the client will send client profile to the administrator for approval. If the administrator was there client request will be active on the administrator side. Once the administrator become online he sees the notification and approves the clients if request is geniune. After the approval administrator will send distinct password for each registered client. The client can login using that password. Once the client login it get group key automatically for group chat. If he preffer single chat no key is used. After login the client page then for the same group members will automatically get the group key for the group chat of the same user. When any of the two group members of the same group will be online that time only it will generated group key otherwise if it is not there thesamegroupmembersinthegroupauthenticationthenitwillnot generatethe group key for the communication.

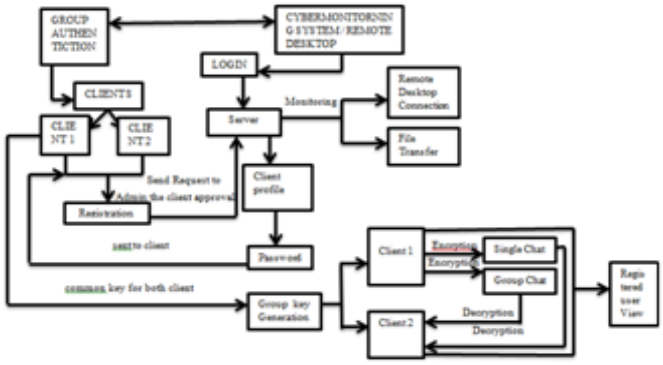

Figure 1. The proposed system of the Group authentication and Cyber Monitoring System

In the client authentication page it can be view as register/ update the client , single chat , clients chat room . After getting the group key then the client can enter the client chat room. During transferring the message from one client to another client the message will be encrypted using the client to another client the message will be encrypted using the RSA algorithm with a symmetric key and does decryption at the receiver side. Both encryption and decryption are done automatically. In the case of single chat user can chat with particular person of the same group member by giving user name of the client. Here also encryption and decryption process will be same as the group chat room. In register page it is used for update the details of the client if the user want to change. These are activities can be update in the key generation page of the administrator side. These are procedure for the group authentication when the message / confidential information will be shared between the clients and server.

In cyber monitorning system activity done in the administrator side, remote desktop connection is done with the administrator system and file. In the remote desktop connection with the help of ip address of the client .By giving the ip address of the client it will display client desktop in the administrator system .The administrator can monitor the client desktop and if client doing any malpractice then administrator can give the warning message to the client then also didn't response the message of the administrator, then administrator can shut down the client desktop. The administrator can view the client desktop details. Registered ip address of the client can only transfer the file.

IV. SYSTEM IMPLEMENTATION

A. *Module description*

1) *Group Authentication Protocol*

In group authentication module both client and server are authenticated. In group authentication client side client has to register the profile with some details like address, username, country, state, mobile number and fill the group which is need for the client for the communication. Then there is a client ip address is registering profile it will automatically display when the client try to register. It will show from which ip address of the client has registered the profile and finally client desktop name also automatically generated. After completing registration client will send the filled profile to the administrator for the approval. Now adiministrator can identifying from which ip address client has requested for the approval. After verifying the profile it will send the password key and username of the client send to the client page. By using the username and password client can log into the log in page. For doing group chat minimum two group members should be online at a time. Here both the client will get group authentication key for group chat. Every time a new member becomes online. Key freshness happened and a new key is given to new member. They can also transfer the files and message using the same key among group member. While transferring the message every message automatically encrypts and decrypt using RSA algorithm so that the unauthorized person cannot seen.

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 viewing the server has to give the ip address of the client. Then display the desktop of the client in the server desktop and it monitor it. In that there are many options like client details that is get information about the client desktop and other options like memory information, screenshots, CDdrive open and close, installed programs, messaging from one desktop to other desktop, restart, log off and shut down finally close.

In case of the file transferring, registered client can be send the file to the other register ip address in the network. Supporting GUI will ease path selection and file selection. Once path and file is selected the selected files send to the receiver.

The whole system based on authenticated key exchange protocol with ip address of the client as one of the security aid and RSA algorithm as the other one .The system communication take place over secure network with increased communication security.

V. ANALYSIS AND RESULT

A. *Security Analysis*

Table 1. Security Analysis of the Proposed System

ATTACKS	DEFINITION	PROPOSED SYSTEM	
		Allow	Deny
Brute Force Attack	A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN)	x	✓
Insider attack	An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access.	X	✓
Replay Attack	A replay attack is a category of network attack in which an attacker detects a data transmission and fraudulently has it delayed or repeated.	X	✓
Masquerade Attack	A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.	X	✓

Security of computer network is needed to fulfil users' requirements of computer network's integrity and confidentiality. With different computer usage, the need of

computer security nature could be divided into different risk levels based on the use, in order to protect the security of computer network and analyse specific security feature based on specific requirements. Proposed system is not vulnerable to attacks like brute force attack, Insider attack , Replay attack and Masquerade attack. Since it is users authenticated key exchange protocol and RSA algorithm and ip address monitoring. Here at the time both the users come on online that time only particular group key is generated. For this each users have registered IP address when registering the client profile so that when the group is generated it only used to the corresponding users that can be monitored by administrator. Only the registered IP address used by client can enter the group authentication page. So the proposed system protected the data/ communication from these attacks above mentioned. Since key is protected and it use authenticated key exchange protocol. The proposed system, is not vulnerable to replay attack and fake id entity problem. Used of Registered ip address as one of the security aid will add on security to above mentioned problem. Thus we can justify that our proposed system is much more secure than existing system.

B. Performance Comparison

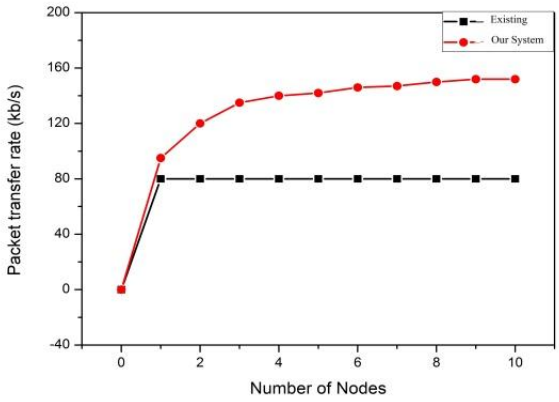

Figure 2. Packet Transfer Rate.

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

C. Encryption and Decryption Time Comparisons of Node Data Security

The parameters for data encryption and decryption for the node data and time con sumption are improved. While increasing the number of the node and time for data transmission is also improved and reduced time delay. In Figure 3 give comparison between existing system and proposed over improvement in transmission time for more amount of data during encryption. In Figure 4 give comparison between existing system and proposed system.

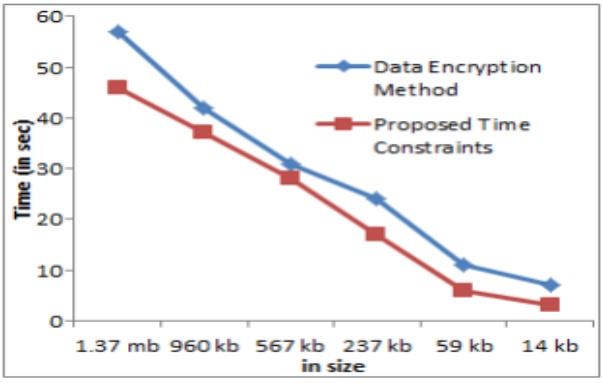

Figure 3. Data Transmission time comparisons with encryption method

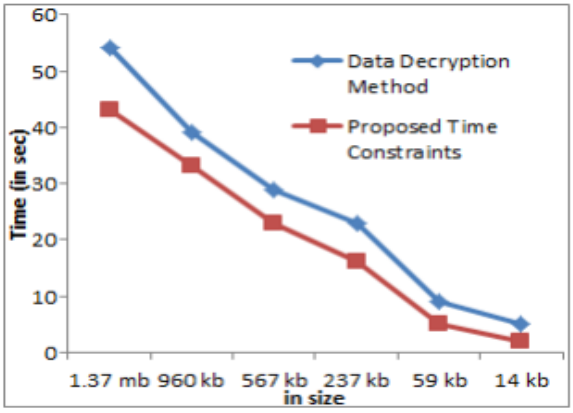

Figure 4. Data Transmission time comparisons with encryption method.

In the proposed system when the size of the encrypted data will be high but there time constraint will be less when compare with the existing system time delay between node network will be high. In the proposed it will reduced the delay between the node of the network improvement in transmission time for more amount of data during decryption. The decryption method in the proposed system it will be reduced the delay time between the node of the network where as compare with the existing system in the network the delay time will be very high and packet size also high so that much delay occur in the existing but in the proposed system even though the system of data will be more then also the time delay is reduced and decrypt within in the minimum number of time and provide that much security for decrypt.

VI. CONCLUSION AND FUTURE SCOPE

D. Conclusion

Here authentication is done using authenticated key exchange protocol, both single and group communication. During message and file transferring the contents are encrypt and decrypt automatically using RSA algorithm with asymmetric key . One of the speciality is that chat can communicated each other with there registered ip address .Only this ip address is used as one of the security aid when the communication take place .Here key freshness also take place automatically key freshness take place after particular time period . The time delay of the communication is also reduced for maximum size of the data in both encryption and decryption side as compare with the existing system. Here authentication is done using are 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 are used for encryption and decryption and file transferring ,ip address, browsing etc .

The remote desktop viewing / cyber monitoring the administrator can view and manage each and every client desktop who is registered with its ip address .It can also identify unauthorized client with this ip address .The developed software is tested well with sample data and outputs obtained according to the requirements. The performance of the system is evaluated, and is found to be efficient. Though it could not be claimed that my project is an ideal project, it will meet the enhanced security requirements.

E. Future Work

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 withsmart cards,” Comput. Secur., vol. 24, no. 8, pp. 619-628, Nov. 2005

[2].M. L. Das, A. Saxena, and V. P. Gulati, ”A dynamic ID-based remote userauthentication scheme,” IEEE Trans. Consum. Electron., Vol. 50, no. 2, pp.629631, 2004.

[3].S. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, and M. K. Khan, ”An enhanced privacy preserving remote user authentication scheme with provablesecurity”, 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. Commun., DOI10.1007/s11277-016-3745-3, 2016.

[5].S. Chaudhry, ”A secure biometric based multi-server authentication scheme for social multimedia networks”, Multimed 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”, Multimed Tools Appl., DOI 10.1007/s11042-016-39211,2016.

[7].F. Wen, and X. Li, ”An improved dynamic ID-based remote user authenticationwith key agreement scheme,” Computers and Electrical Engineering, 38(2):381387, 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 SystemSciences, 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 ed, 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 ComputerConf.,Vol.48,pp.313317,1979.

[17].A.Shamir,” How to share a Secret “,Comm ACM, Vol.22, no.11,pp.612-613,197922

[18].Qi Xie, Duncan S. Wong, Guilin Wang, Xiao Tan, Kefei Chen and LimingFang ”Provably Secure Dynamic ID-based Anonymous Two-factor Authenticated Key Exchange Protocol with Extended Security Model”, IEEE Transactions on Information Forensics and Security, DOI 10.1109/TIFS.2017

