Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure LAN messenger and File Transfer Application

Santhosh Kumar B.J
M.Tech, Amrita Vishwa Vidyapeetham,
Mysore Campus, Mysore, India

Abstract: Offline Secure chat with message transfer Application over LAN enables a user to connect with a fellow user and send and receive encrypted messages to the other user. This application is totally secure for the users. Only if the receiver has the key he can decrypt the ciphered message to the correct message. Users can also transfer files from one system to another using this application. The advantage of using this simple LAN messenger is that no active internet connection is required. The need of a centralized server is also not required.

Keywords: GUI, FTP, TCP

I. INTRODUCTION

Online Chat Application contains all the information about the system and how it works. This contains a user level description of the project, along with a detailed list of prioritized requirements and a brief description of change management process thereafter. Our system enables a user to connect with a fellow user and send and receive encrypted messages to the other user. This application is totally secure for the users. Only if the receiver has the key he can decrypt the ciphered message to the correct message. Users can also transfer files from one system to another using this application.

1) Allows a user to send and receive encrypted messages using a symmetric key.
2) Secure file transfer between peers using this application.

This contains a user level description of the project, along with a detailed list of prioritized requirements and a brief description of change management process thereafter. Our system enables a user to connect with a fellow user and send and receive encrypted messages to the other user. This application is totally secure for the users. Only if the receiver has the key he can decrypt the ciphered message to the correct message. Users can also transfer files from one system to another using this application.
In this application, encrypting a message protects the privacy of the message by converting it from plain readable text into cipher text. Only the recipient who has symmetric key used to encrypt the message that can decipher the message. This is separate process from digitally signing a message. This application provides a GUI for sending encrypted message and decrypting them with the right key. The message sent by the sender is encrypted and sent to the receiver and the message is decrypted at the receiver side and displayed to the receiver. The advantage of using this simple LAN messenger is that no active internet connection is required and no need of a centralized server.

II. SYSTEM ARCHITECTURE

- The Software product has two main components one sender machine and one client machine.
- PC connected to each other using IP address over Wi-Fi. Both PC's are connected to each other using LAN cable. User enters the IP of PC which is connected to the system through LAN. Fig: Cloud Storage Verification.
- The sender can receive texts in both secure format and in simple format. User can perform secure communication and file transfer.

All interaction with the user takes place through a single GUI requires following steps.
Main modules of the system.

- **Connection Establishment**: The sender and receiver have to be connected to each other using a LAN cable connected using different TCP/IP and FTP protocols. Connection establishment includes the sender sending connection request to the receiver and the receiver approving the connection request.
- **Simple messenger**: Sending simple text message from one user to another.
- **Secure Messenger**: Sending a cipher message which is encrypted using a symmetric key DES algorithm and a private key from one system to another.
- **Decryption:** Decrypion of messages at the receiver side using the private key which is used to encrypt the data at the sender side.
- **File Transfer:** Transfer of file from one system to another using FTP

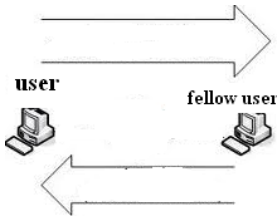

Fig1. Simple architecture

General Structure

- The Software product has two main components one sender machine and one client machine.
- PC connected to each other using IP address over Wi-Fi.
- The sender can receive texts in both secure format and in simple format.

Procedural Approach

- Both PC's are connected to each other using LAN cable.
- User enters the IP of PC which is connected to the system through LAN.
- Chat user can perform chat, file transfer.

All interaction with the user takes place through a single GUI.

Connection Establishment: The sender and receiver have to be connected to each other using a LAN cable connected using different TCP/IP and FTP protocols. Connection establishment includes the sender sending connection request to the receiver and the receiver approving the connection request.

- **Simple messenger**: Sending simple text message from one user to another.
- **Secure Messenger**: Sending a cipher message which is encrypted using a symmetric key DES algorithm and a private key from one system to another.
- **Decryption:** Decrypion of messages at the receiver side using the private key which is used to encrypt the data at the sender side.
- **File Transfer:** Transfer of file from one system to another using FTP.

Fig 2: sender creates a plain text input.

Figure3.Receiver decrypts the message using private key.

III. CONCLUSION

All the activities provide a feeling like an easy walk over to the user who is interfacing with the system. All the disadvantages of the existing system have been overcome using the present system of "**iLanChat"** which has been successfully implemented at client's location. A trial run of the system has been made and is giving good results.

The system has been developed using Microsoft Visual Studio in C#. All the modules are tested separately and put together to form the main system. Finally the system is tested with real data and everything worked successfully. Thus the system has fulfilled the entire objective identified. The system has been developed in an attractive dialogs fashion and the entire user interface is attractive and user friendly and suits all the necessities laid down by the clients initially. So user with minimum knowledge about the computers and the system can easily work with the system.

IV. FUTURE ENHANCEMENT

This Project can be further enhanced by including file encryption by selecting the best available cryptographic algorithms and multiple user chat. This will help the users to send encrypted files and to chat with multiple clients connected using a switch or hub.

To provide Usage of High security cryptographic Using Blowfish algorithm, which is 448 bits key length results in higher security, rather than using traditional DES and AES algorithms are smaller in key sizes results in lesser security. Data Integrity can be achieved by selecting best message authentication algorithms like SHA-1 or MD5.Intrusion detection can be achieved.

REFERENCE

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. EUROCRYPT*, 2005, pp. 457–473.

[2] V.Goyal, O. Pandey,A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Computer and Communications Security*, 2006, pp. 89–98.

[3] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in *Proc. CRYPTO*, 2010, pp. 191–208.

[4] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," *Theor. Comput. Sci.*, vol. 422, pp. 15–38, 2012.

[5] B. Chevallier-Mames, J.-S. Coron, N. McCullagh, D. Naccache, and M. Scott, "Secure delegation of elliptic-curve pairing," in *Proc. CARDIS*, 2010, pp. 24–35.

[6] B. G. Kang, M. S. Lee, and J. H. Park, "Efficient delegation of pairing computation," *IACR Cryptology ePrint Archive*, vol. 2005, p. 259, 2005.

[7] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in *Proc. NDSS*, San Diego, CA, USA, 2005.

[8] A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," Ph.D. dissertation, Israel Inst. of Technology, Technion City, Haifa, Israel, 1996.

[9] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proc. EUROCRYPT*, 2011, pp. 568–588.

[10] N. P. Smart and F. Vercauteren, "On computable isomorphisms in efficient asymmetric pairing-based systems," *Discrete Appl. Math.*, vol. 155, no. 4, pp. 538–547, 2007.

[11] J. B. Nielsen, "Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case," in *Proc. CRYPTO*, 2002, pp. 111–126.

Software Engineering: A Practitioners approach- Roger.S.Pressman

2. Professional Android

3. Application Development- RetoMeie

4. An Introduction To Database Systems -Bipin.C.Desa

5.Database system concept –Silberschatze

