Secure Communication in Intranet

Prof. Bharati Kale[1], Mr. Abhijit B. Kawade[2], Mr. Sharad T. Pawar[3], Mrs. Supriya Ghanekar[4]
[1, 2, 3, 4] Department of Computer Engineering
[1, 2, 3, 4] DPCOE, Wagholi

Abstract- *Aiming at the security requirement of the Intranet that is different from Internet and security architecture for Intranet is proposed. This proposed system, secure communication in intranet network, which is used to improve secure digital communication for specific number of terminals, ranges from 500 and above. This system proposed communication medium such as audio, text chat and file transfer. Technology used java as frontend and SQL as backend. This system provides the database for maintaining the previous communication data, and focusing on faster communication medium. This proposed system providing the complete package for communication (audio chat, text chat and file transfer). The purpose of a providing security is the combination of the general security services, such as Authentication, Confidentiality, Integrity or Non-repudiation. Security is achieved by Rijndael algorithm, where data and operations performed on data get secured. Proposed system is based on self pop-up notification window if terminals are online or offline, this is help to notify user.*

Keywords- Intranet security, Cryptography, Secure digital communication.

I. INTRODUCTION

Currently, most enterprise intranet systems process uses information for security and access it for authentication purposes. Aiming at the security requirement of the Intranet that is different from Internet and security architecture for Intranet is proposed. Security switches are used to connect each separate part of the Intranet, based on application as well as user authorization control to carry out network access control. The security architecture focuses on security guarantee of intranet inside the traditional network boundary, and provides foundation framework to Intranet security which can ensure the reliability, usability, confidentiality, integrity, and maneuverability of the Intranet.[1] However, this information is often captured by unauthorized users who may edit, modify, delete or otherwise corrupt this data. Cryptography is used to prevent unauthorized access and modification of data through the intranet. This technology proposes an efficient security procedure that incorporates a new model that allows flexible web security access control in securing information over the intranet. It further improves the security access control by providing authentication corresponding to different security page levels relevant to public ownership and information sensitivity between different enterprise departments. This approach reduces processing time and prevents information leakage and corruption caused by mistakes that occur as a result of communication protocol errors between clients PC's or mail security methods. An intranet uses network technologies as a tool to facilitate communication between people or work groups to improve the data sharing capability and overall knowledge base of an organization's employees. Intranets utilize standard network hardware and software technologies like Ethernet, Wi-Fi, TCP/IP, LAN[6]. Intranet does Secure Connection of computers using Internet Protocol (IP) to share resources within an Organization. Security typically consists for a number of terminals such as computers or other devices, which are communicating through digital channels. Protection against all possible threats is too expensive; therefore here we are using algorithm names as Rijndael [11]. Designed under certain assumptions about the attacks, Rijndael based on permutation substitution method which is faster in encryption and decryption of data and reduce time complexity of performance. The aim of a providing security is the combination of the general security services, such as Authentication, Confidentiality, Integrity or Non-repudiation [3]. We also discuss information security threats surrounding Intranets and methods of protection against these threats. The use of Intranets as internal information transmission channels within organizations serves to emphasize the importance of their secure realization. Information security threats between Intranets and other networks and information systems are rather similar. Information security solutions in Intranets are based both on experiences gained from the Internet and on new solutions designed particularly for Intranets. Special areas of interest within Intranet security are communications between two or more nodes, file transmission, audio chat and text messages, data and operations security [8]. User can access within the organization network and cannot be access outside organization network. This application provides interface between two or more system in network. The facilities are as; secure electronic file transfer between two or more system that has become essential for organization transactions and communication. This system allows effective and efficient communication, allowing immediate receipt of acknowledgment or reply, colleagues can send and reply instant message in real time without face to face, and meanwhile the work report can be shared during the instant

chat session. Also, audio communication within the network is provided along with conferencing option. Some other features available are: 'Group Messaging' in text messaging, 'Conference call', and 'Call Recording' in this system.

II. WORKING

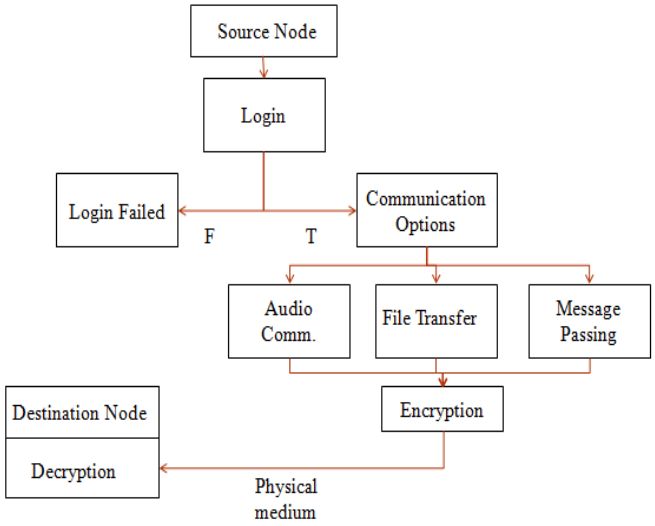

Figure 1: Data flow diagram

The above Figure 1 is the data flow diagram for secure communication in intranet network [4]. In this diagram, when a user wants to communicate with another user by using software firstly he needs to login by a valid username and password [3]. After completion of login, there is a client list which is maintains in database by using My SQL. The client list is nothing but the IP addresses of systems. The application is running on those systems then these systems will be shown as online. If user wants to communicate with any other system then select any client from Client list and select communication medium as per user interest. There are three communication options: First is the Audio Communication, second is the File Transfer and last is the chatting. User can use one of them. If users select audio communication then the communication request is made to selected client and at the client side received a notification like ringing. If client accept the request then the connection is established and is start communication. After starting communication the data is encrypted by using algorithm and sent to receiver by physical medium. After receiving data on the receiver side, the message is decrypted and made available to the receiver. If user want to communicate more than one user then conference is possible. If user select file transfer option then one to one file transfer and broadcasting is also possible. The user select a file which want to send then the file is send to the selected user. The connection establishment and encryption, decryption process is same as the audio communication. The file is received and notification is generated. If user selected the chatting option then one-to-one and, one-to-many chatting is possible. Further procedure is same as file transfer option. The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria, the block sizes can mirror those of the keys[13]. Rijndael uses a variable number of rounds, depending on key/block sizes, as follows: 9 rounds if the key/block size is 128 bits, 11 rounds if the key/block size is 192 bits, 13 rounds if the key/block size is 256 bits. Thereafter, there are Nr-1 rounds and then the final round[12]. The transformations form a State when started but before completion of the entire process. The exact transformations occur as follows: the byte sub transformation is nonlinear and operates on each of the State bytes independently - the invertible S-box (substitution table) is made up of 2 transformations. The shift row transformation sees the State shifted over variable offsets. The shift offset values are dependent on the block length of the State.

III. PROPOSED WORK

System adopts browser/server structure. Server and client is side a PC with headphone and microphone is needed. The chatting contents are forwarded through browsers, and point to point connection is directly established between browsers during audio and text chatting, file transfer. The Working structure [6] is shown in Figure 2.

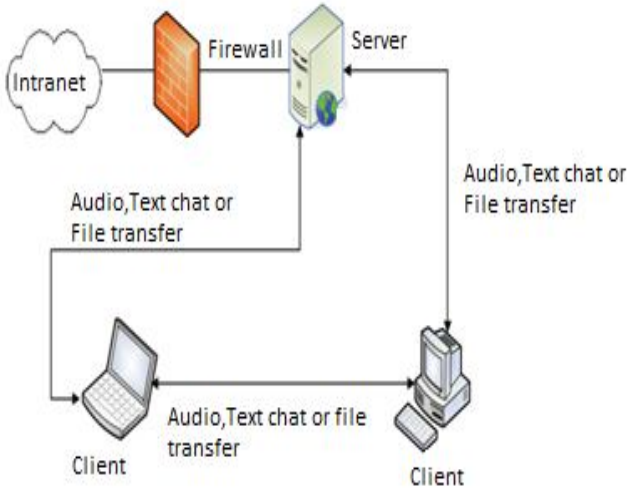

Figure 2: Working structure [6]

A. Login Module

Information required for registration is very simple, only including username and password Login successfully will show the online client list. . After logging in, user able to use communication option like audio and text chatting, file transfer.

B. Text chat module

In chatting module, Tomcat 7 is adopted on server side for realizing Socket. Text chatting is realized through Socket technology based on java. A monitor activated by server side is needed for monitoring connection requirement sent by using peer to peer connection. The connection with server is established through calling constructor of Socket. After receiving connection from client side, server side creates Message in order to serving for this client side. If the above-mentioned steps are completed, Socket is on OPEN state, and the messages could be sent to server by calling the send function of Socket.

C. Audio Chatting

The collection, sending and display of audio on client side is realized through adopting receiving call, which could traverse the interconnection between two nodes. Using the programming interface provided by WebRTC, the transmission of audio could be realized. Headphone and microphone could be activated when calling performs. Binary data stream of audio could be acquired.

D. File transfer

In File transfer module, Tomcat 7 is adopted on server side for realizing Socket. FTP (file transfer protocol) is the protocol which helps to transfer the file. Using the file transfer module client have to select file path and attach them for sending it to the receiver. Receiver will get the notification as they received the file or if they are offline.

IV. RESULTS AND ANALYSIS

→ Software	Secure Communication in Intranet Network		IP Messenger	Aspera
↓ Modules	Before Encryption	After Encryption		
File Module	13-15 mb/s for 10/100 Ethernet	9-11 mb/s for 10/100 Ethernet	10-12 mb/s for 10/100 Ethernet	10 mb/s for 10/100 Ethernet
Message Module	3.10/3.20 Beta	3.30/3.40 Beta	3.42/3.50 Beta	3.52/3.60 Beta
Audio Module	Instantly	Instantly	No	Instantly

This is the system which helps to improve the digital communication within a specific range of terminals. Here each employee who works for organization consist of some sort of authentication, on that basis user will get it. Now comparing with the existing software, our software is more reliable to use and handle it. It provides the complete package to the user, as we mention there audio chatting, message transfer and file transfer on same portal. In the audio chat user can perform peer to peer or conference call. After choosing the appropriate user those who are online, ringing facility is there for making call. In message passing user can perform one to one or group chatting, within it user also able to broadcast the message and it will transfer to the user if they are not online. File transfer module comes with sending file one to one or many. Our software is based on self pop-up notification window if they are online or offline. Most common talk about the security and that is maintain by the Rijndael algorithm. This algorithm used for the encryption and decryption of data i.e. in the form of text, audio or file while communicating. Here we are setup our software where LAN connection in already establish so that no any extra expense for communication.

Now considering existing systems, some of LAN i.e. intranet messenger applications are mostly based on "Announcement mode". Another popular LAN messenger that lets you perform some office or workplace chat tasks. This application helps you to uphold workflow in your circle atmosphere, but has limitations to make the group chats or broadcast them. Only single module for audio transmission, text chats and files transfer. But this system provides combination of Audio, message and file. Here we also deal with the transferring and receiving speed of data. Intranet security is the major part, i.e. maintained by allowing only authenticated people to enter into the system.

V. CONCLUSIONS

Test results show that this chatting system could be applied to various network environments, providing chatting service for different types of people, and the system is safe by using Rijndael, efficient and easy to maintain and extend. Advantage of our system is no announcement mode, ringing with pop up window facility is provided. This system has various advantages over the already available systems; the complete package for communication (audio chat, text chat and file transfer) is available for the user.

REFERENCES

[1] GrantDavidson, Louis Fielder and Mike Antill, "HIGH-QUALITY AUDIO TRANSFORMS CODING AT 128 KBITS/S"Dolby Laboratories, Inc.100 Potrero Avenue San Francisco, California.

[2] Makoto Takizawa, Hiroya Mita, "Secure Group Communication Protocol for Distributed Systems" Dept. of Computers and Systems Engineering Tokyo Denki University Ishizaka, Hatoyama, Saitama 350-03, JAPAN, 1993.

[3] Chen Tieming, Chen Huibing etc. Designing and Implementing New Dynamic Web Password Login Method, Computer Applications and Software, 2011, 28(7):31-34.

[4] Misun Yu, Woosuk Cha, Jun-Keun Song, "Design and Implementation of an Audio/Video Group Chat Application for Wireless Mesh Networks" Electronics and Telecommunications Research Institute, January 2013.

[5] Benjamin Tobler. "A Structures Approach to Network Security Protocol Implementation", a Dissertation, Faculty of Science, University of Cape Town, 2005.

[6] W. Richard Stevens, TCP/IP ILLUSTRATED Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols[M], China Machine Press, 2011.

[7] Raju Ramaswamy, "Secure Data Communication in Local Area Networks" Computer Science and Telecommunications Department University of Missouri - Kansas City 5100 Rockhill Road, 2011.

[8] Hamid Boland and Hamed Mousavi, "SECURITY ISSUES OF THE IEEE 802.11B WIRELESS LAN" Carleton University-2004.

[9] M. Chaudhari and K. Saxena, "Fast and Secure Data Transmission using Symmetric Encryption and Lossless Compression," Int. J. Comput. Sci. Mob. Comput., pp. 58–63, 2013.

[10] J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Springer-Verlag, Berlin Heidelberg, 2002.

[11] H. Gilbert and M. Minier, A collision attack on seven rounds of Rijndael, Proceedings of the 3rd AES Candidate Conference, pp.230-241, April 2000.

[12] S. Lucks, "Attacking seven rounds of Rijndael under 192-bit and 256-bit keys," Proceedings of the 3rd AES Candidate Conference, pp. 215-229, April 2000.