RESEARCHERID
THOMSON REUTERS

[Rohilla, 6(6): June 2019] ISSN 2348 – 8034
IDSTM-2019 Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SECURE IMPLEMENTATION OF TELEPRESENCE, SHARED WHITEBOARD AND WEB TOURS TO EXISTING TEXT, AUDIO AND VIDEO CONFERENCING SYSTEM

Charu Rohilla
Computer Science Department, Ganga Technical Campus, India

ABSTRACT

The aim of this paper is to introduce the new system extended from the existing system. The existing system is text, audio and video conferencing system which is using socket programming. For communication in the existing system TCP and UDP protocols are used and communication takes place in the form of streams. The system is using Session Initiation Protocol for connection establishment, modification and termination. The extension to this system is the introduction of telepresence, shared whiteboard and web tours. Telepresence is a complete type of web conferencing, which typically includes three large curved screens, and a fourth screen above the rest for displaying shared work. Shared whiteboard is similar to actual chalkboard where anything written or drawn on the virtual board are shared with all individuals participating in conference. Web tours Supports a group of people all browsing the web with a single person acting as a tour guide. The individual designated as the "tour guide" navigates the websites, etc. while the rest of the conference participants are able to follow along and view identical websites. Security is one of the primary concern on internet to incorporate it into the system various encryption and decryption algorithms are used.

keywords: *IP, TCP, UDP, SIP, VoIP, API, TU, UA, JAR,SC,AC,OBS.*

I. INTRODUCTION

Conferencing is the activity of talking to people in different places using phone or computer systems. conferencing provides transmission of static images and text between two locations. Conferencing means communication between three or more speakers at different locations. There are different types of conferencing. The text, audio and video conferencing is already implemented in the existing system. The new implementation is of shared whiteboard, telepresence and web tours features implementation to the system with security.Whiteboarding is the placement of shared files on an on-screen shared notebook or whiteboard. With this type of software, several people can work on the image at the same time, each seeing changes the others make in near-real time. Telepresence is the use of virtual reality technology, especially for remote control of machinery or for apparent participation in distant events. It is a sensation of being elsewhere, created by virtual reality technology.Telepresence refers to a set of technologies which allow a person to feel as if they were present, to give the appearance of being present, or to have an effect, via telerobotics, at a place other than their true location.Web Tours is a sample Web-based travel agency application used to demonstrate how LoadRunner is used as a solution for performance testing.With these features security get also implemented with in the system. Security introduces the concept of encryption and decryption process to provide secure conferencing systems. This process uses the symmetric key encryption algorithms to implement security. The implementation of system uses the socket programming. To provide communication between users it uses the TCP & UDP protocols inaddition to SIP protocol. For this the system uses Jitsi which is a free and open sourcemultiplatform voice VoIP, videoconferencing and instant messaging applications.

II. SHARED WHITEBOARD

White boarding is the placement of shared files on an on-screen shared notebook or whiteboard. With this type of software, several people can work on the image at the same time, each seeing changes the others make in near-real time. Electronic whiteboarding was included at least as early as 1996 in the CoolTalk tool in Netscape

Navigator 3.0.An interactive whiteboard (IWB) device can either be a standalone computer or a large, functioning touchpad for computers to use.

A device driver is usually installed on the attached computer so that the interactive whiteboard can act as a Human Input Device (HID), like a mouse. The computer's video output is connected to a digital projector so that images may be projected on the interactive whiteboard surface.

The user then calibrates the whiteboard image by matching the position of the projected image in reference to the whiteboard using a pointer as necessary. After this, the pointer or other device may be used to activate programs, buttons and menus from the whiteboard itself, just as one would ordinarily do with a mouse. If text input is required, user can invoke an on-screen keyboard or, if the whiteboard software provides for this, utilize handwriting recognition. This makes it unnecessary to go to the computer keyboard to enter text.

Thus, an IWB emulates both a mouse and a keyboard. The user can conduct a presentation or a class almost exclusively from the whiteboard.

In addition, most IWBs are supplied with software that provides tools and features specifically designed to maximize interaction opportunities. These generally include the ability to create virtual versions of paper flipcharts, pen and highlighter options, and possibly even virtual rulers, protractors, and compasses—instruments that would be used in traditional classroom teaching.

Uses for interactive whiteboards may include:

- Running software that is loaded onto the connected PC, such as a web browsers or other software used in the classroom.
- Capturing and saving notes written on a whiteboard to the connected PC
- Capturing notes written on a graphics tablet connected to the whiteboard
- Controlling the PC from the white board using click and drag, markup which annotates a program or presentation
- Using OCR software to translate cursive writing on a graphics tablet into text
- Using an Audience Response System so that presenters can poll a classroom audience or conduct quizzes, capturing feedback onto the whiteboard.
-

Fig-1 Information radiator

III. TELEPRESENCE

Telepresence refers to a set of technologies which allow a person to feel as if they were present, to give the appearance of being present, or to have an effect, via telerobotics, at a place other than their true location.Telepresence requires that the users' senses be provided with such stimuli as to give the feeling of being in that other location. Additionally, users may be given the ability to affect the remote location. In this case, the user's position, movements, actions, voice, etc. may be sensed, transmitted and duplicated in the remote location to bring about this effect. Therefore information may be traveling in both directions between the user and the remote location.A popular application is found in telepresence videoconferencing, the highest possible level of videotelephony. Telepresence via video deploys greater technical sophistication and improved fidelity of both sight and sound than in traditional videoconferencing. Technical advancements in mobile collaboration have also extended the capabilities of videoconferencing beyond the boardroom for use with hand-held mobile devices, enabling collaboration independent of location.

Fig- 2 A telepresence video conferencing system

IV. WEB TOURS

Web conferencing may be used as an umbrella term for various types of online collaborative services including web seminars ("webinars"), webcasts, and peer-level web meetings. It may also be used in a more narrow sense to refer only to the peer-level web meeting context, in an attempt to disambiguate it from the other types of collaborative sessions.[1] Terminology related to these technologies is inexact, and no generally agreed upon source or standards organization exists to provide an established usage reference.In general, web conferencing is made possible by Internet technologies, particularly on TCP/IP connections. Services may allow real-time point-to-point communications as well as multicast communications from one sender to many receivers. It offers data streams of text-based messages, voice and video chat to be shared simultaneously, across geographically dispersed locations. Applications for web conferencing include meetings, training events, lectures, or presentations from a web-connected computer to other web-connected computers.

V. PLAYFAIR CIPHER ALGORITHM

The playfair cipher is a symmetric encryption technique. The scheme was invented in 1854 by Charles Wheatstone but bears the name of Lord Playfair who promoted the use of cipher. The technique encrypts pair of letters. It uses a 5 by 5 table containing a phrase or keyword. To generate the key table first fill in the spaces in the table with the letters of keywords, then fill the remaining spaces with the rest of letters of alphabet in order. The technique encrypts pairs of letters (bigrams or digrams), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. The frequency analysis of bigrams is possible, but considerably more difficult. With 600[1] possible bigrams rather than the 26 possible monograms (single symbols, usually letters in this context), a considerably larger cipher text is required in order to be useful. The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.

To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "J" or "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.

To encrypt a message, one would break the message into digrams (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD". These digrams will be substituted using the key table. Since encryption requires pairs of letters, messages with an odd number of characters usually append an uncommon letter, such as "X", to complete the final digram. The two letters of the digram are considered opposite corners of a rectangle in the key table. To perform the substitution, apply the following 4 rules, in order, to each pair of letters in the plaintext:

- If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any letter, itself uncommon as a repeated pair, will do.
- If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
- If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
- If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.
- To decrypt, use the inverse (opposite) of the last 3 rules, and the first as-is (dropping any extra "X"s or "Q"s that do not make sense in the final message when finished).

ISSN 2348 – 8034
Impact Factor- 5.070

P	I	R	A	T	E
4	2	0	J	L	1
D	Z	H	7	C	W
3	O	6	M	Q	U
V	K	B	5	G	9
F	Y	N	X	8	S

Keyword:PIRATE420

6X6 MATRIX PLAYFAIR CIPHER

Fig-4 Playfair cipher matrix with keyword 2

VI. RESULT ANALYSIS

We have implemented a secure communication system. For the implementation of system eclipse is used.
1. The Fig below shows all the communication methods in the system like text, audio, video and screen sharing.

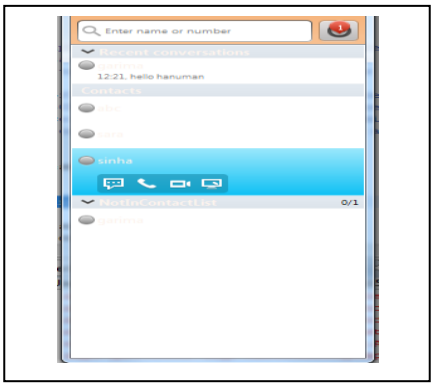

Fig-5 communication methods

2. The Fig below shows the call from one person to another

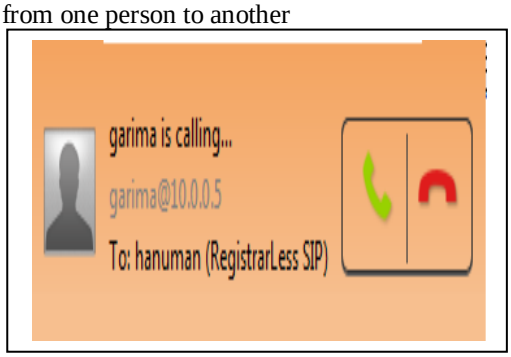

Fig6-Call from one person to another

ISSN 2348 – 8034
Impact Factor- 5.070

3. The Fig shows a person who is online.

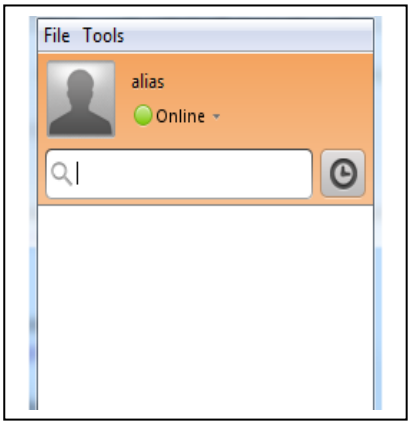

Fig7- Online

4. The Fig shows the call history and has parameters like-

- Time of calls
- Type of calls
- Person with which call was made.
- All call history stored with login ID.

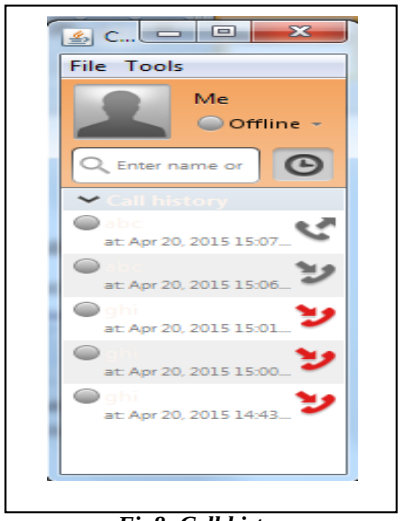

Fig8- Call history

5.The Fig 6 below shows the file menu and its options are:

- Add new account
- Add contact
- Quit

ISSN 2348 – 8034
Impact Factor- 5.070

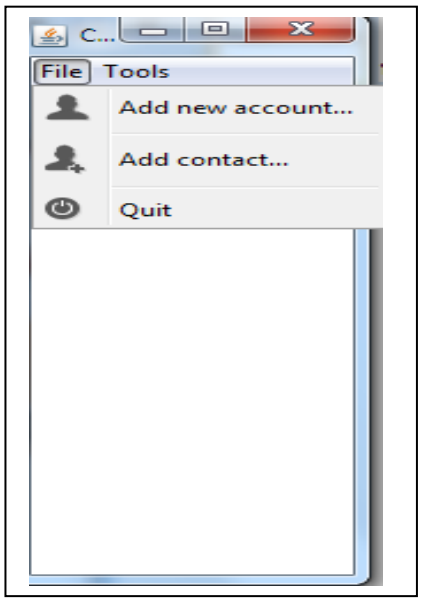

Fig9- File Menu

6.The Fig 7 below shows the Image capture from webcam.

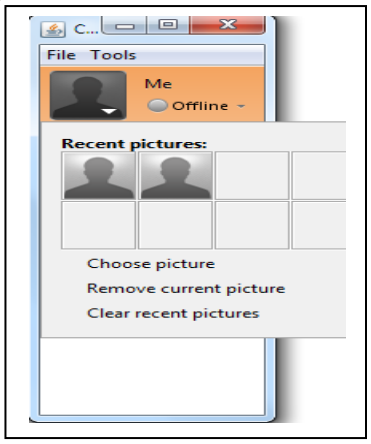

Fig 10: Picture Option

VII. CONCLUSION

In this system modification to existing system has been done. The former system was text, audio and video conferencing system. The new system includes the concept of telepresence, shared white board and web tours implementation. The new system uses the symmetric key algorithm to provide security for the system.It avoids the participants having to spend time travelling to meet each other. It is the technology that allows you to hold meetings with several correspondents who are located in different places while seeing and talking to them in real time. Conferencing reduces Travel Time and Costs, Optimised Attendance, Increased Productivity, Employee Retention & Sustained Competitive Advantage. The system uses the TCP & UDP protocol to provide communication using socket programming. In addition to this the system is also uses SIP protocol which uses JITSI software for communication.

REFERENCES

1. *Sumedha Kaushik, Ankur Singhal published by International journal of advanced research in computer science and software engineering. Network Security Using Cryptographic Technique.*
2. *Mr. Nisarga Chand, Mr. Bappadittya Roy, Mr. Krishanukundu published by International Journal Of Advanced Research In Computer Science And Software Engineering.*
3. *Qingzhang Chen, Zhongzhe Tang, Yidong LI, Yibo NIU.Jianhua MO published by Journal Of Computer Information Systems. Research on Encryption Algorithm Of data Security.*
4. *Liancheng Shan Niang. Research on security mechanisms of SIP based VoIP systems.*
5. *Arup Acharya, Nilanjan Banerjee. Session Initiation Protocols:Impact and Implications.*
6. *Jaideepverma, Inderjeet Singh Behi. Research paper on Java swings.*
7. *MiroslavVoznak, Jan Rojhon. Methodology for SIP infrastructure performance testing.*
8. *Jitsi. Wikipedia, the free encyclopedia.*
9. *https://vitaenterprisesolutions.com.au/new-ideas/articles/6-benefits-online-video-conferencing*