International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 3, May-June 2015 **ISSN 2278-6856**

New Approach for Security Chatting in Real Time

Dr. Alaa Kadhim , Sura Khalaf

Computer science department

Abstract

Chat is to participate in a synchronous text, video, audio, image, or exchange of information with one or more people over a computer network. There is the need to ensure confidentiality of communication to breed honest and frank chatting free from fear of eavesdropping and breach of privacy. A Secure Chat System is a system which enhances communication between two or more people within an organization or over the internet in a way that seriously attempts to be free from risk of interception by or involvement of unauthorized persons.In this project a new proposal for secure chatting system is constructed for wired and wireless communications. This system permits user to keep the secrecy for data and services and ensure general safety. In spite of challenge and attacks on computer communication, the proposed chatting system uses new approach of block cipher algorithm to achieve peer- to-peer security for each communication connection. It is designed to limit attacks and overcome these challenges.This system consists of two parts: the first part is concerned with the server, the systems begin to start connection between subscribes, key generation, dynamic key distribution and ensure that this subscriber is registered in the system. While the second part is concerned with the security of data and services by encryption these data and services using the proposed new approach of block cipher algorithm. The proposed chatting system is to provide secure environment for chatting and speed of data transmission using new approach of block cipher and anther service can use the stream cipher for encryption to get fast more than standard method (ASE) and proposal, in addition to programming the system with modern programming language platforms c#.

Keywords: Encryption, Decryption, Advanced Encryption Standard, bee colony, magic, data encryption standard.

1. Introduction

Internet-based text message applications are one of the most common means of communicating today. As a matter of fact there are several varieties of chatting. The simplest computer chatting is a method of sending, receiving, and storing typed messages with a network of users **[1]**. This network could be WAN (Wide Area Network) or LAN (Local Area Network). Our chatting system will deal only with LAN's and it is made up of two applications one runs on the server side (any computer on the network you choose to be the server) while the other is delivered and executed on the client personal computer. Every time the client wants to chat he runs the client application, enters his user name, host name where the server application is running, and hits the connect button and starts chatting. For this system to be physically realized you should be familiar with programming and networking **[2]**. "windows sockets" is our programming interface to have access to network functionality **[3]**. This paper introduces design and implementation of new approach for secure chatting in real time, this system provides several service for user's communication with each other.

2. Secure multimedia communication

With the rapid progress in information technology and an enormous amount of media appearing over Internet, for example, text, audio, speech, music, image, and video. Several pivotal challenges include copyright protection, integrity verification, authentication, and access control. As a consequence, the subject of security protection in multimedia communication has attracted intensive research activities in academia, industry, and government.Guaranteeing information security is becoming increasingly important **[4]**. Multimedia data like images, audios, or videos are different from plain text. They are often of large volumes and are compressed in order to save the storage cost and bandwidth. Due to such requirement and property, the media protection mechanisms for images, audios, or videos are significantly different from the ones for text or binary data. Taking video encryption, for example, maybe only sensitive part in video data are encrypted while the other parts are left unencrypted in order to improve the encryption efficiency and reduce the encrypted data volumes. Furthermore, to keep compliant with communication, the synchronization information in video data should be left unencrypted, for example, package header. In the aspect of video authentication, the malicious tampering should be detected while the acceptable operations like recompression can be ignored. With the recent advances in network and multimedia technology, the applications in commercial scenario become increasing crucial. There is an increasing trend in the multimedia content distribution from the central service provider to the individuals, for example, video-on demand, Internet Protocol television, and Peer-to-Peer sharing. In these applications, piracy is becoming a critical issue. Solutions are needed to protect the copyright of multimedia content. During the past decades, schemes have been reported for secure multimedia communication, for example, key management, multimedia encryption, authentication, digital fingerprinting, access control, and digital rights management. These techniques are able to protect multimedia content's confidentiality, integrity,

ownership, traitor traceability. In addition, in different networks such as Internet, 3G wireless and Peer–to-Peer, different secure protocols and algorithms are required to provide the system security. All these topics are in active development **[5].** Additionally, devices likedigital cameras, mobile/video phones, graphics processing unit.Need to be equipped with such security mechanisms. In these situations, software solutions may not be adequate to provide high real-time performance.

3. Proposal New Scenario for Session Start and Key Generation

Start main server to establish the log-in and key generation and dynamic distribution and use voice chat, text chat, video chat, image and file transfer and wait for clients requesters, client gets IP for server pc from file administrator and shares it and connects to main server to get access to login after connected if client registers in proposed system he just enters user name and password to log-in to get all service else if client does not register he can creates account in proposed system and the request is sent as array of byte server, checksfirst byte if the first byte number is 8 then the client can log-in request else if the first byte number is 7 then client create account request then stores client information in database then server checks user information to create the Account then inform user about creating his account and show message(The new account created successfully). If the client registers logs-in to request server pass to access. Give the permission to use all other services then show message. (Access Granted) then client Select any Friend to Get Pair Session Key from server. Then it sends request Ask for Pair Session Key with first byte numb 9, server Wait for Request for Session Key the server Generate New Pair Session Key (Using Developed scheme mixing between Geffe and Hadamard Key generation Methods) and Send it to Both Users (U1 & U2) ,Wait for New Users (Account or Login) or another Request for Session Key or using chat Services, Extract the Pair Session Key Received and store it with the Friend ID to use it with all their Conversation, Connect to Any Service (Voice, Video, and Chat) on Ports: (4530, 4531, and 4532) respectively with Selected Friend to start a Conversation, server check port client send it and then connect to service then Start Using Services with selected & Connected Friend, figure (2) procedure between server and clients.

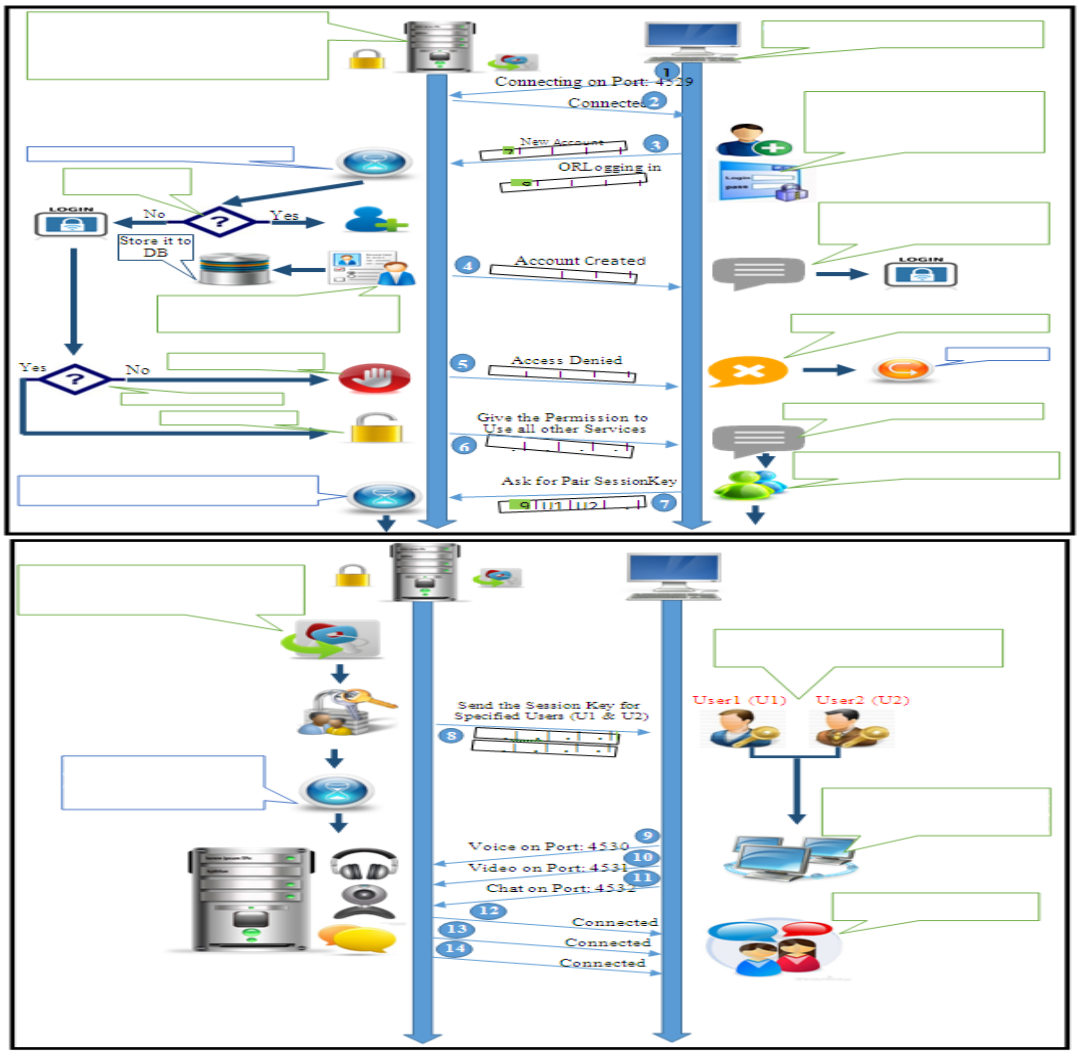

Figure (2): Session Started and Generate & Share Secret Keys

4. Send/ Receive Scenario

The user can login to his account using user name and password and select friend from friend list and select service (text chat, video chat, voice chat and any transfer type of file), the service selects subscriber encryption using proposed new block cipher (advanced encryption standard) [6] this proposed algorithm used new s-box depend on A.I bee colony [7] and sends them to the web service .the last web service receives encryption service then decryption service. Figure (3) shows send and receive service

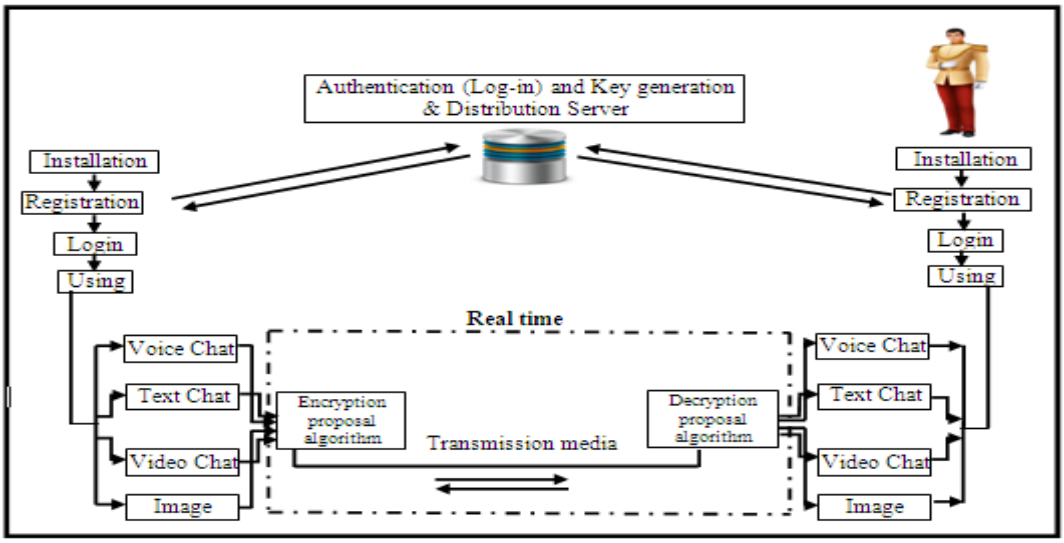

Figure (3): Scenario Send / Receiving

5. System Services

The actual operator of secure chatting system consists of four services, text chat, video chat, voice chat and transfer file, they will be summarized in turn:

- **Text chat service:**
  It is most important service today everyone wants to connect to other for exchange of information or learning, he provides the encrypted message to be transmitted, the proposed new approach for block cipher is used.
- **Video chat service:**
  Wants to connect to other for exchange of information or learn by webcam or gets online lectures, he provides the encrypted frame to be transmitted, the proposed new approach for block cipher or stream cipher is used.
- **Voice chat service:**
  It provided the encrypted voice to be transmitted, the proposed new approach for block cipher or stream cipher used.
- **Transfer file service:**
  everyone wants to connect to other for exchange of information or transfer any type of file (pdf, wave, doc, image, zip, etc.) he provides the encrypted file
  to be transmitted, the proposed new approach for block cipher or stream cipher is used.

6. System Implement

Whenadministrator starts to run web conference server , the server takes IP of PC and then administrator sends PC IP as text file for all PC connected with it, depending on Wi-Fi or Lan cable, all pages of proposed system are displayed in web browser using Silverlight .Figure(4) shows web conferencing servers.

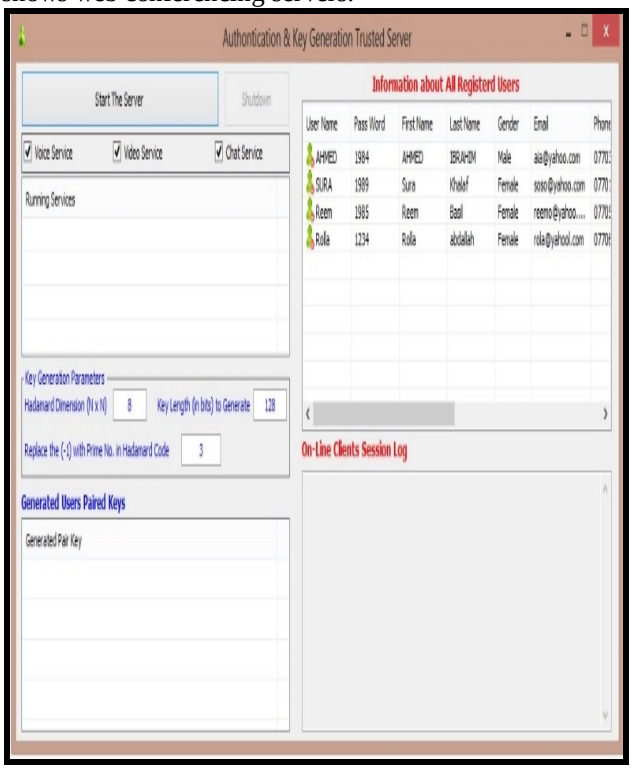

Figure (4): Web Conferencing Server

After web conferencing server is debugged the server lists PC of IP and assigns port of all services and generates distribution key using two layer algorithm generator of Hadamard matrix and Geffe generator described in previous chapter and server

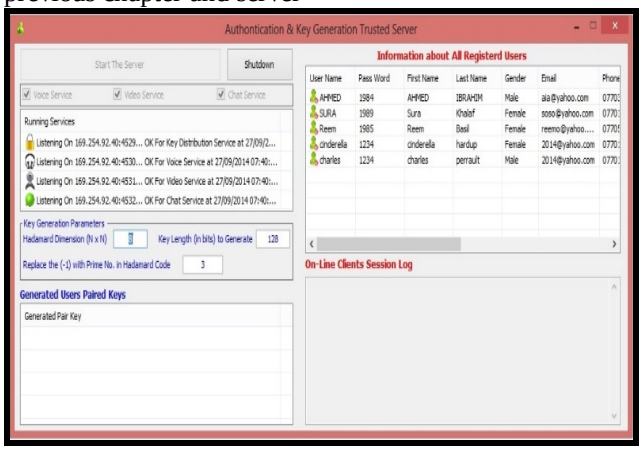

Figure (5): Show Start Web Conferencing Server

The user can enter to the system but must use file receive from administrator server and write server IP in file then press connect for authentication server bottom then automatically enable two bottom login and register and then users use the user name and password. When the user enters user name and

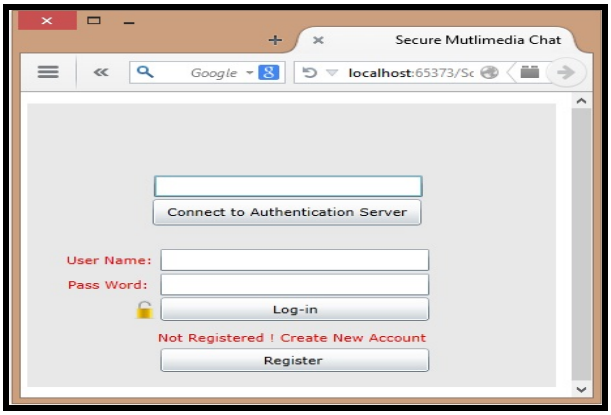

Figure (6): Login Page

If the user is not registered he presseson register bottom to enter next page called create account page .Figure (7) shows create account page

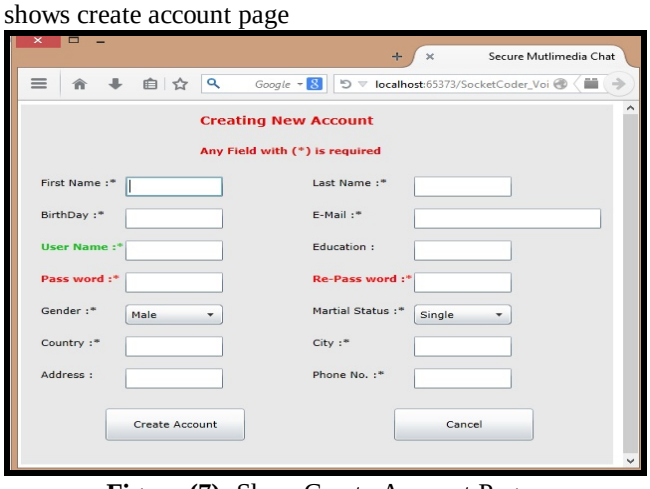

Figure (7): Show Create Account Page

After he fills all fields in create account the user presses create account bottom then all information is sent automatically to server, the server checks information if the information is true it sends message to user "user account was created successfully, please log-in using your user name and password" and if the user does not want register in system, he can press cancel bottom and exit system, Figure (8) shows fill page create account.

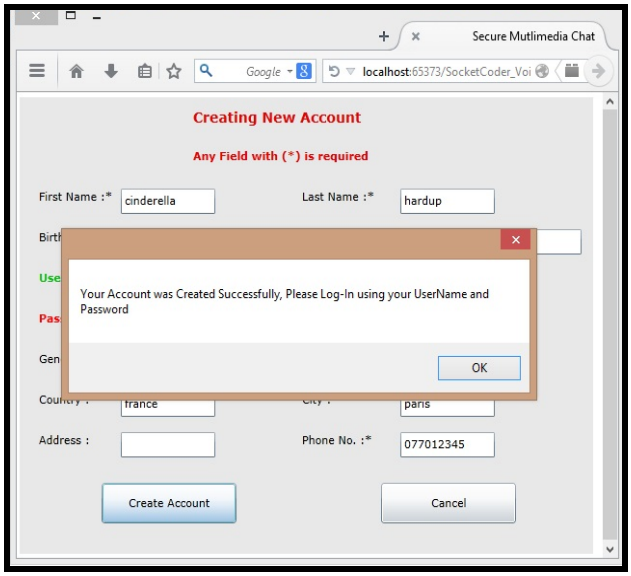

Figure (8): Fill Page Create Account

But status of user called Cinderella in server is offline now if Cinderella login status her in server is online, Figure (9) shows user status in server

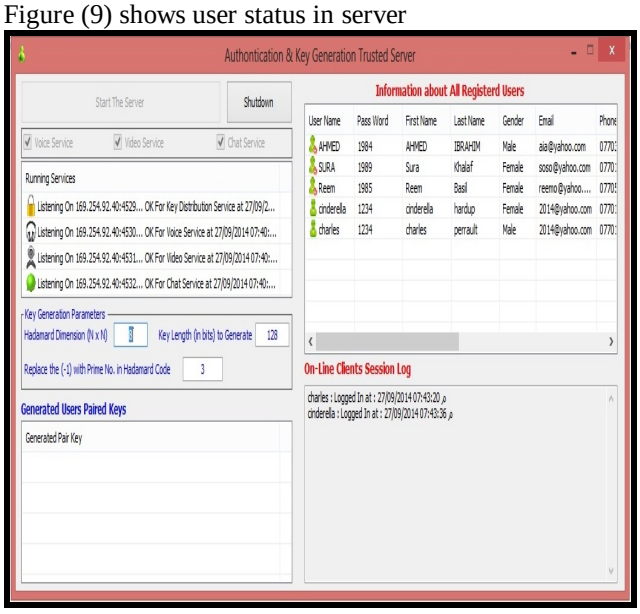

Figure (4.10): User Status in Server

Now the user is registered in system and can enter to the next page, this page firstly welcomes the user or subscriber and offers four options, user selects what services to connect with other user selected from friend list, service connect consist of text service, voice service or video service. Figure (10) show welcome page.

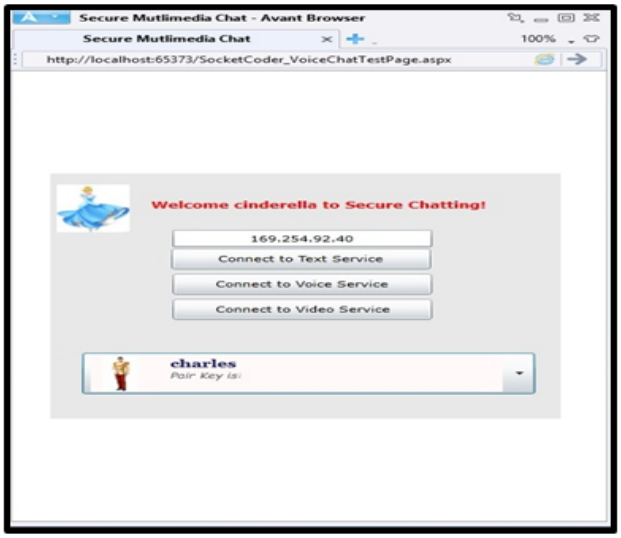

Figure (10): Welcome Page

Now the user is name Cinderella is login in the system, the status server is changed after Cinderella register. Figure (11) shows web conferencing server status after user logins and shows pair key is generated between two users registered in the system. User can select any option she wants chatting and selects friend from friends list but on condition the friend chosen is registered in the system. Figure (12) shows connect to text service.

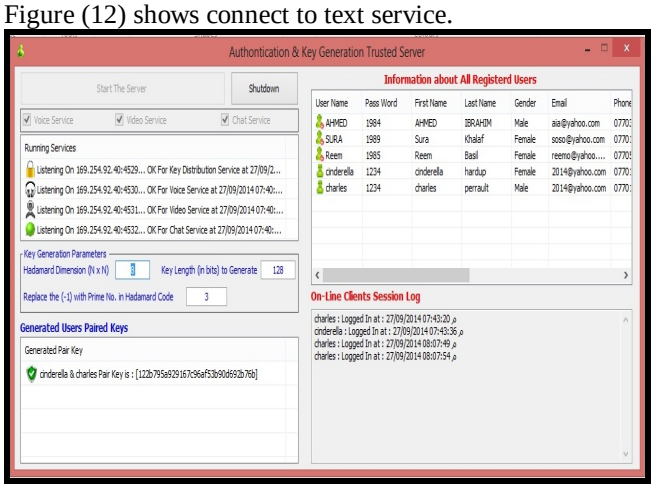

Figure (11): Web Conferencing Server Status after User Register

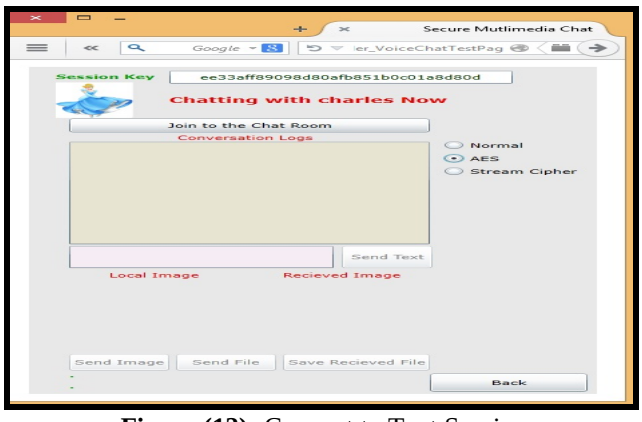

Figure (12): Connect to Text Service

Cinderella after selecting Charles from friend list server which generates pair key and sends to Cinderella and Charles key for encryption and decryption and massage for send and receive, then Cinderella presses join the chat room to enable bottom, then her select, algorithm for encryption of message or file send, Figure (13) shows message

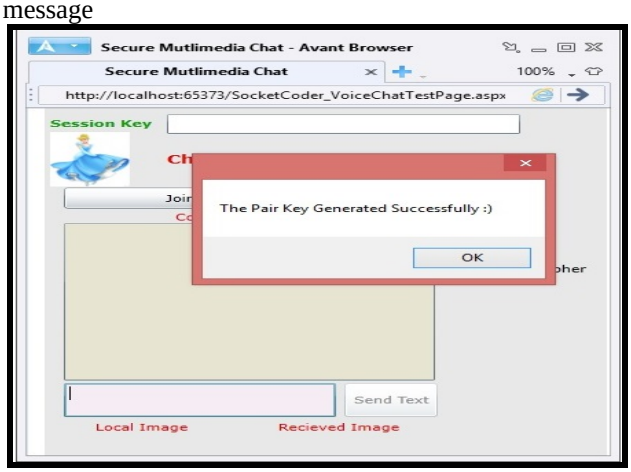

Figure (13): Message Generate Pair Key

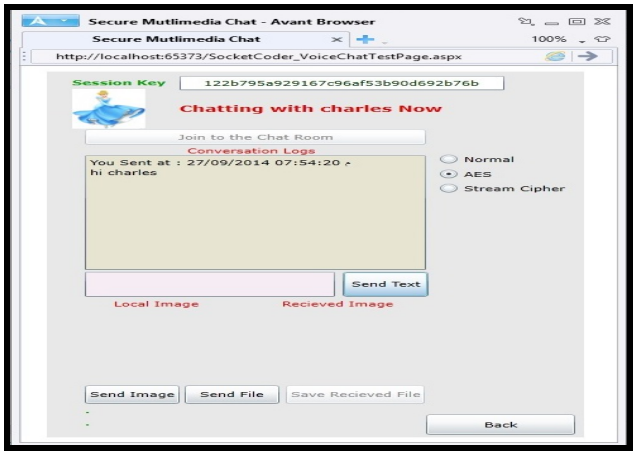

Figure (14): Send Text Message

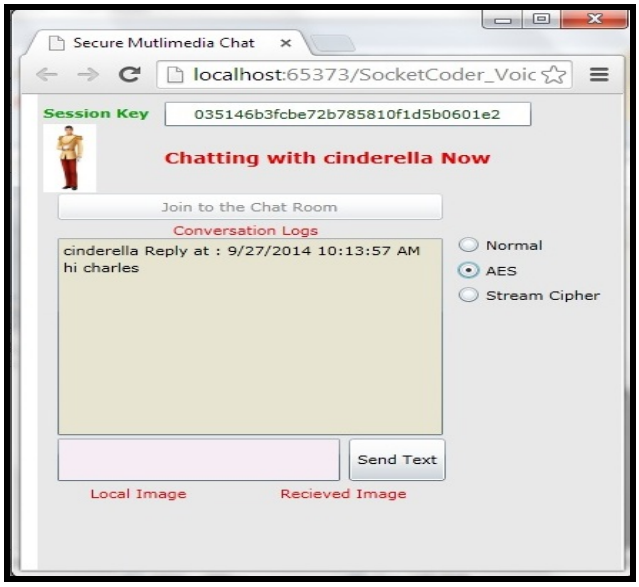

Figure (15): Receive Text Message

When Cinderella wants to send image or any type of file to Charles she can press on send image or press on send file then she open his computer to get image from folder in Cinderella pc save image or

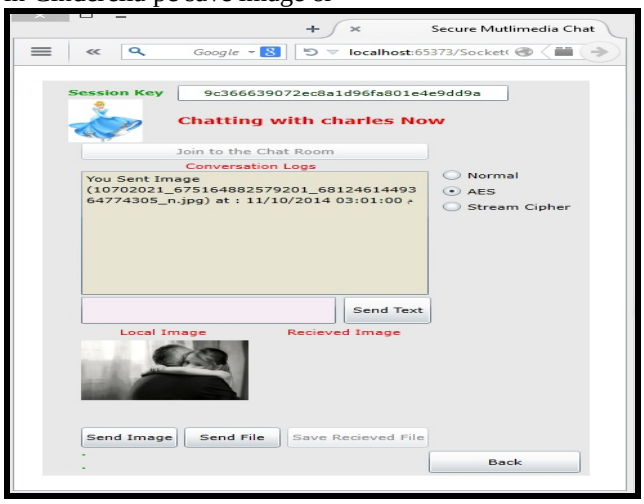

Figure (16): Send Image or File

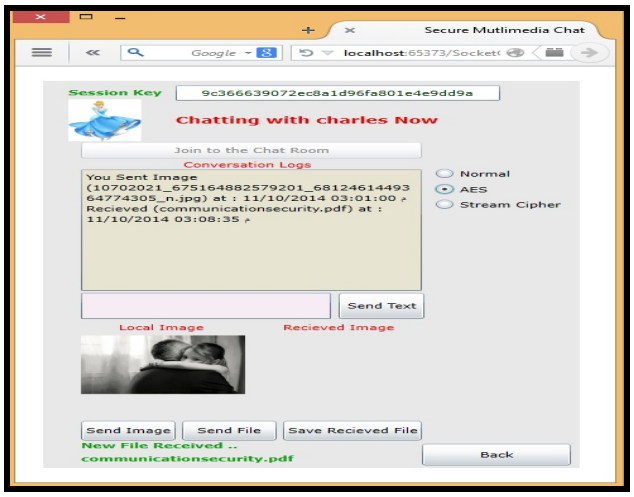

Figure (17): Receive Image

When Cinderella wants to connect through video server with Charles she can press bottom back to back welcome page and presses connect to video service to enter to video chat page .In video chat page Cinderella can select algorithm for encryption

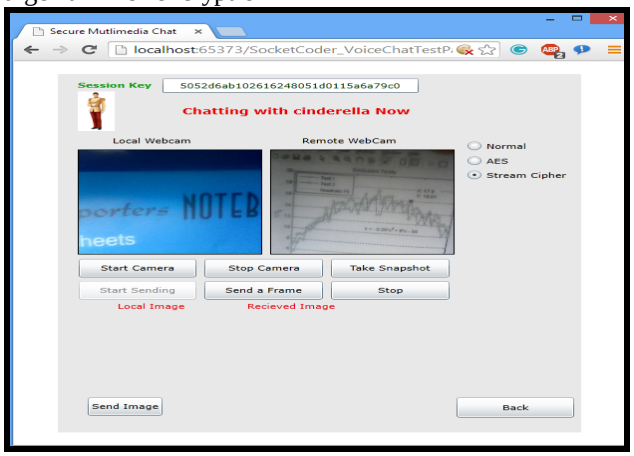

Figure (18): Send Video Frame

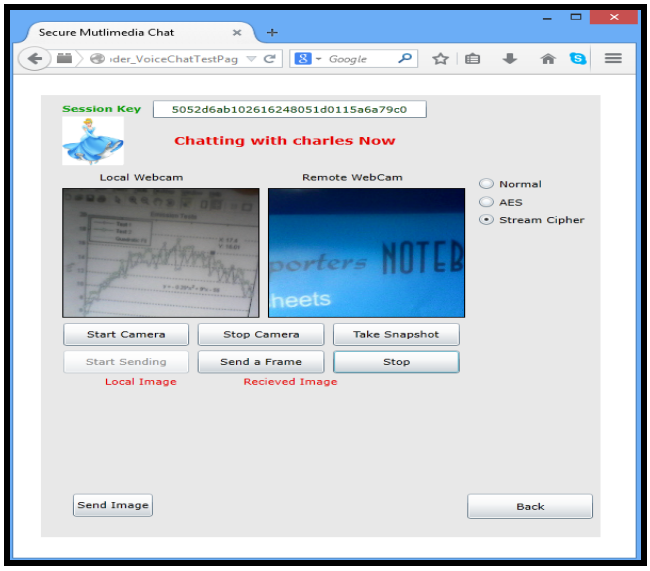

Figure (19): Receive Video Frame

When Cinderella wants to connect through voice server with Charles she can press bottom back to back welcome page and presses connect to voice service to enter to voice chat page .In voice chat page Cinderella can select algorithm for encryption and decryption and then presses start the

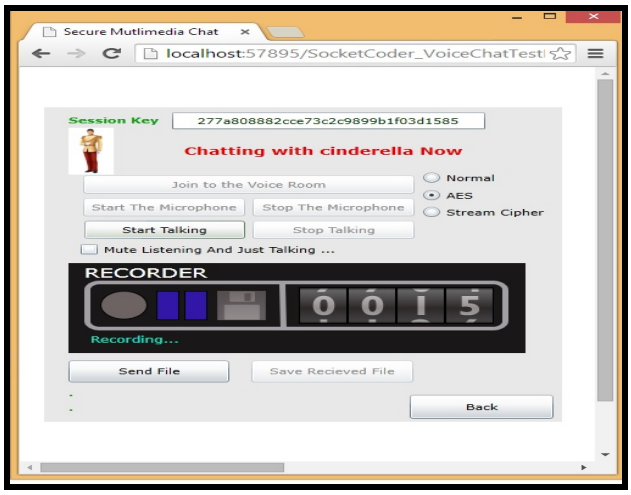

Figure (20): Recording

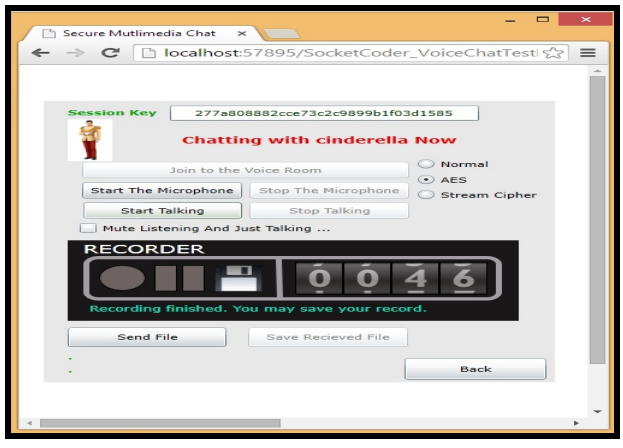

Figure (21): Save Recording

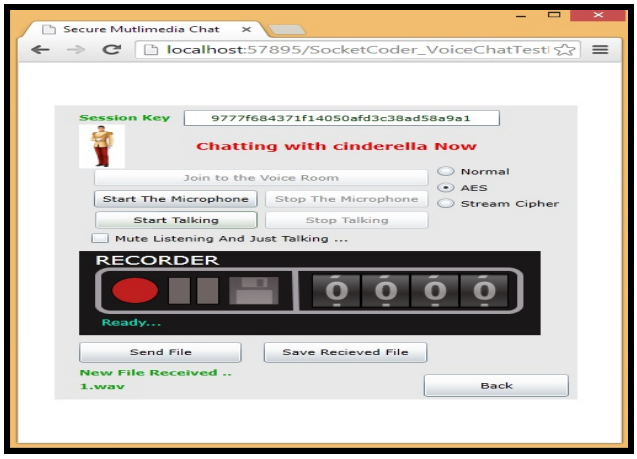

Figure (22): Receive Recording

When Cinderella wants to start chat with other subscribers in the proposed system she can go back to welcome page and select other subscribers then selects service connect, the web conferencing server status changes firstly on-line client session log now shows three subscribers or client online and generate users paired key side now it shows pair key between Cinderella and Charles and Cinderella and Sura.

7.Conclusion

The proposed system manipulates in an elegant manner the communication and data transfer process by enhancing the secrecy in communication. Several conclusion are reached through design security chatting system. The items shown below represent the important conclusions which are drawn from the proposed system

- The proposed new idea generates dynamic S-Box and dynamic inverse S-Boxusing best algorithm artificial bee colony to enhance static original S-Box and its inverse to increase confusion and complexity for attacks compared with original.
- The proposed new idea for reordering technique in state depends on row and column (magic rotate) static shift row depends on row only to increase diffusion.
- Linear operation in add round key layer is replaced to special function for increasing complexity on attacks.
- The proposed new approach generate key by using two nonlinear generators to get huge secret key.
- The original (AES) and proposed methods cause some delay time so put the stream cipher method for sending data less important quickly from the (AES) original and proposed method.

Reference's

[1]. Hervé.C, Laurent.V,"Net.lang Towards the multilingual cyberspace",IDRC / CRDI, Canada, 2012.
[2]. Waleed.F. "DEVELOPING ACHAT SERVER",Notre Dame UniversityFaculty of Natural and Applied Sciences Department of computer Science, 2000.
[3]. Frank. S," A QoS Architecture for Open Systems ", Ph.D. ThesisDepartment of Computer Science Trinity College, University of Dublin December 1999.
[4]. Manuel .C,Los .A,Gustavo .C," The Network Society from Knowledge to Policy",Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005.
[5]. Shiguo.L, Peter.S ,"Introduction to special issue on secure multimedia services", springer , September 2010.
[6]. Alaa.K, Sura.Kh,"New Approach of Block Cipher Using A.I", Iraqi association of information technology, university ofMustansiriya, 2014.
[7]. Alaa.K, Sura.Kh,"Propsal New S-Box for AES Algorithm Depend on A.I Bee Colony",Eng. and Technology journal, university of technology , 2014.