**MINOR PROJECT 1**

**SYNOPSIS**

**ON**

**Secure Client Server Chat Application**

**Submitted By**

|  |  |  |  |
| --- | --- | --- | --- |
| Ashish Pandey | Mridul Thapa | Nikhil Mishra | Surabhi Raj |
| 500063104 | 500060077 | 500062584 | 500063663 |
|  |  |  |  |

***Under the guidance of***

**Mr. Pushpendra Kumar Rajput**

Assistant Professor

Department of Cybernetics,

School of Computer Science

upes-new-logo

**Department of Cybernetics,**

**School of Computer Science**

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**Dehradun-248007**

**Month- 2018**

**Project Title: Secured Client-Server Chat Application**

**Abstract:**

This presented algorithm is mainly designed for having a secure file transfer in the low privilege servers and as well as in a secured environment too. This methodology will be implemented in the data center and other important data transaction sectors of the organization where the encoding process of the software will be done by the database administrator or system administrators and his trusted clients will have decoding process of the software. This software will not be circulated to the unauthorized customers. The system comprises of an Encryption algorithm that is RSA which consists of two keys Public and Private. If one key is used at the encryption side, another key of same user should be used at decryption side. We have to first find the public and private keys and after that the data will be encrypted and decrypted.

**Keywords:** RSA, Key length, prime number, public key, private key, cipher text, plain text

**Introduction:**

Instant messaging has been a boon to the computer industry and is now thoroughly used in contrast to email or other archaic form of technologies. There has been a rapid increase of these kind of services in the market, but the loopholes are the same. While wirelessly transmitting a message it is prone to the security gaps. For message encryption there has been 2 kind of encryption being used: Asymmetric and Symmetric Encryption. Asymmetric encryption provides the public key and private key, the RSA Algorithm is a type of it. RSA has been the more secure algorithm for encryption, but is also not very good at handling longer strings.

In order to send or receive a message, the server socket is attached to a port, from where it transmits. The project contains the user level description of the project, the requirements of the project, and a study of PERT chart thereafter.

The application helps a user to connect to someone and send & receive encrypted message to and fro. This application helps to convert a message in plain text to a message in ciphered text which can only be accessed by the recipient who has the symmetric key to the message. This guarantees the privacy of the data that is being shared. This GUI application helps in encrypting and decrypting a message and is not digitally signed. The advantage of this application is sending and receiving of the messages with encryption can be done without any active internet connection, as we are using simple messenger, and taking down the need of a centralized server.

**Literature Review:**

A socket is a standard connection protocol that supports data correspondence over the system between terminals that are connected. The standard connection bolsters the information transmission both by the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) conventions between the terminals. TCP is a transport layer protocol utilized by applications that require ensured conveyance of information. Essentially, it is a connection-oriented protocol. To convey over TCP one initially need to set up a connection between pair of sockets, where one socket is a customer and another has a place with the server. After the connection is set up between them then they can speak with one another. [1]

A client is a system that gets to or wants for an administration made available by a server. A server is a system (hardware or software) program racing to aid the request service of other system programs. Port is a software instrument that enables the brought together associated Servers to tune in for solicitations made by customers. Port is really purposed as a door to tune in for the mentioned parameters by the server terminals or different machines. It is a software address on a system that is on the network. Whole request-response continuing among this Application is transported over through machine ports. Secure Sockets Layer convention is utilized for encryption of information for secure information transmission. IP is the sensible system address of a gadget on a system. It is notational called dotted-decimal. [2]

It is increasingly helpful to use peer-to-peer application since it works legitimately to the client. The communication to the servers destroy excess time whenever varied with the peer-to-peer. That is the reason distribution is increasingly liked to be utilized for the chat system as the fundamental strategy and further as an alternative technique, to utilize particularly with the end goal of the feature of transferring a file. [3]

RSA is one of the most successful, asymmetric encryption systems today. Originally discovered by the British intelligence agency GCHQ, it received the classification “top secret”. We have to thank the cryptologists Rivest, Shamir, and Adleman for its civil rediscovery in 1977. They stumbled across it during an attempt to solve another cryptographic problem. [4]

**Problem Statement:**

The Client-Server communication channel is widely used in many applications. These kind of applications usually have a very protected server side, whereas the Client-side are prone to loopholes and can be hacked into by another client.

The client side is always vulnerable to threat attacks, or unauthorized access. The main objective of this project is to develop a Secure Client-Server Chat Application, to provide security measures at both the ends.

**Objective:**

The purpose of this project is to develop a chat application where by instant messages are encrypted with a private key and public key at the transmission end, and decrypted with the same private key at the receiving end on the network using RSA Algorithm.

**Methodology:**

***FrontEnd***

Step 1: CMD on Ubuntu providing the channel to send a message through.

Step 2: A message will be displayed prompting the user to enter the text they want to send and that needs to be encrypted.

Step 2: The text entered by the user will be transmitted after encryption by RSA Algorithm.

Step 4: The text will be received by the user at the other terminal which will be the same text unless data is lost in transmission, i.e. no invalid message will be shown.  
  
***BackEnd***

Step 1: The message entered by the user will be encrypted using RSA algorithm.

Step 2: Public key will help encrypt the message and generate a private key.

Step 3: The private key will be sent along the ciphered message.

Step 4: At the receivers end the private key will be used to decipher the message.

**System Requirements: (Software/Hardware)**

Hardware Interface:

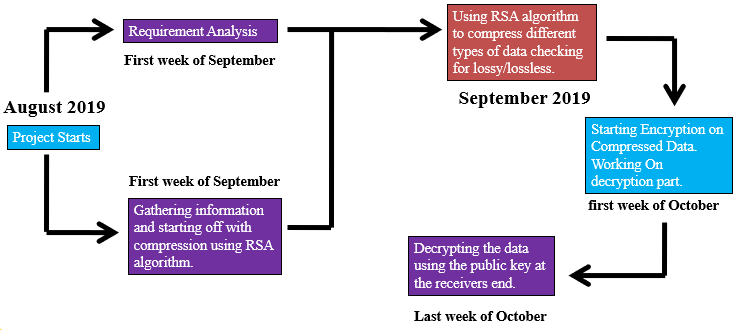
Minimum requirements will be as follows:

1. 128 MB RAM required
2. Processor with speed of 500 MHz
3. Internet or LAN connection

Software interface:

1. Turbo C/C++
2. Notepad editor
3. VM Ware
4. Linux based OS

**Schedule: (PERT Chart)**



**References:**

1. Limi Kalita,”Socket Programming”,*(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4802-4807*.
2. Pranab Bandhu Nath & Md.Mofiz Uddin,”TCP-IP Model in Data Communication and Networking”,*American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN : 2320-0936.*
3. Rushabh Balpande, Chetan Dusane, Khushboo Kashyap & Nandkumar Patil,”Client Server Based Secure Chat Application Using Peer-To-Peer Network Architecture” *International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS) ISSN (Online) 2349-6967*
4. By Dr. Prerna Mahajan & Abhishek Sachdeva,”A Study of Encryption Algorithms AES, DES and RSA for Security”, *Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013 Online ISSN: 0975-4172 & Print ISSN: 0975-4350*

**Approved By**

**Signature Signature**

**Mr. Pushpendra Kumar Rajput Dr. Monit Kapoor**

**Mentor Head of Department**