DESIGN AND IMPLEMENTATION OF MULTI-USER SECURED CHAT APPLICATION USING JAVA SOCKET PROGRAMMING AND RSA

Jahnabi kalita, Shiwani Agarwal, Purnendu Bikash Acharjee

PG Student Department Of Information Technology, School of Computing Sciences,
Kaziranga University, Assam, India
Department Of Information Technology, School of Computing Sciences,
Kaziranga University, Assam, India

Abstract— The aim is to develop a Chat Application using Client Server Architecture which runs on Socket programming provided by java. It is made up of two applications-the client application and the server application, both runs on the users PC without an internet connection. To start a chat client should get connected to the server where it can do public chatting i.e. message can be broadcasted to all connected clients. There can be many clients as there is no limitation and if any new client is added it will show a message. Also, for clients that will be online it will show a message. Now for securely passing the message we have used here RSA encryption algorithm where data will be seen in a encrypted form in the server itself and then the client will receive the decrypted or original message.

Index Term- Client Application , Decryption ,Encryption, Server Application

I. INTRODUCTION

In Multi-User web based Chat application, we are using socket programming in Java. Socket programming in java is use for communication between the applications that is running on different java run time environment. It can be either connectionless or connection-oriented. In
Socket programming client must have the two information, IP address and Port Number of server.

This project is to create a web based chat application with a server and a client to enable the clients to chat with many other clients in the same common chat group. This project is to simulate the multicasting chatting. In case of multicasting when a message is sent to a group clients , then only a single message is sent to the router. The main purpose of this project is to provide Multicasting functionality through network. Also we are trying to implement here an encryption technique to provide better security.

Client Server Communication:

Client/Server communication involves two components. They are client and a server. There are usually multiple clients in communication with a single server. The clients send requests to the server and the server replies to the client requests.There are three main methods to client/server communication. These are given as follows:

Socket:

Sockets are used for communication between two processes on the same machine or different machines. They are used in a client/server model and consist of IP address and port number. There are many application protocols uses sockets for data connectivity and transfer of data between a client and a server.Socket communication is quite low-level as sockets only transfer an unstructured byte stream across processes. The structure on the byte stream is usually imposed by the client and server applications.

Remote Procedure Calls

These are communication techniques that are used for client-server applications. A remote procedure call is also known to be a subroutine call or a function call. The RPC translates the clients requests and sends to the server. This request might be a procedure or a function call to a remote server. When the server request is received, it sends the response back to the client.

Pipes:
These are communication methods that contain two end points. From one end of the pipe data is entered by a process and consumed from the other end by the other process. The two different types of pipes are ordinary pipes but named pipes. Ordinary pipes allow one way communication and two way communication is done by two pipes.

II. METHODOLOGY

The application is designed by using Socket Programming in Java .

We are using socket programming in Java. Socket programming in java is use for communication between the applications that is running on different java run time environment. It can be either connectionless or connection-oriented. In Socket programming client must have the two information, IP address and Port Number of server.

Here we can run several clients simultaneously .Where the server can encrypt all messages excluding the exit and joining message of the client. For Encryption and Decryption we are using RSA cryptography algorithm .

The RSA algorithm is the base of a cryptography , A set of cryptographic algorithms that are used for different security services or purposes — that enables public key encryption and is commonly used to protect sensitive data , especially when it is sent over an unsafe network such as the Internet. The RSA algorithm is an asymmetric cryptography algorithm. Asymmetric Encryption is a type of cryptography where keys come in pairs. Where one key is used for encryption and another key is used for decryption.

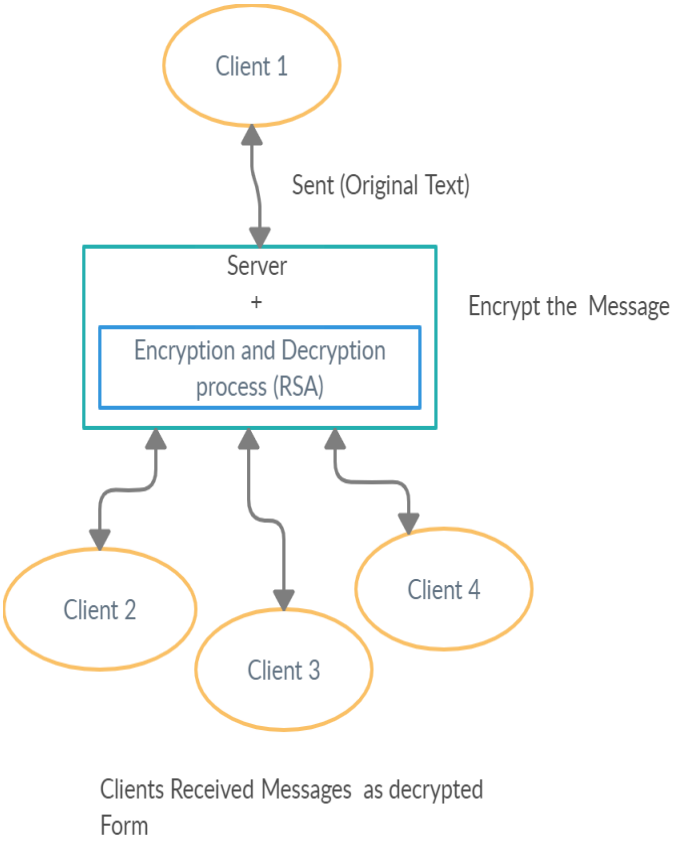

Fig.3. Diagram after using RSA algorithm

RSA Algorithm:

Step 1: Generating the RSA module:
The initial process starts with the selection of two prime numbers, namely p and q, and then the calculation of their product N.

N=p*q

Let N be a large number.

Step 2: Calculate e:
Considering number e as a derived number that should be greater than 1 and less than (p-1) and (q-1) respectively. The primary condition is that there should be no common factor (p-1) and (q-1) except 1.

Step 3: Public key:

The defined pair of numbers n and e forms the public key of the RSA and is made public.

Step 4: Private Key:

Private Key d is based on numbers p, q and e. The mathematical relationship between numbers is as follows:

ed = 1 mod (p-1) (q-1)

The formula above is the basic formula for Extended Euclidean Algorithm, which takes p and q as input parameters.

Encryption Formula:

Consider a sender sending a plain text message to one whose public key is (n, e). Using the following syntax-to encrypt the plain text message in the specified scenario

C = Pe mod n

Decryption Formula:

The method of decryption is very simple, and involves calculation analytics in a systematic approach. The result module will be determined as − provided that the receiver C has the private key d.

Original text = Cd mod n

III. LITERATURE SURVEY

#1: Design and Implementation of an Improved RSA Algorithm.
Yunfei Li, School of Information Science and Engineering, Yunnan University, Kunming, China and Quing Liu,Tong Li ,National Pilot School of Software, Yunnan University,china

Conclusion: Proposed a new RSA variant (which is EAMRSA- Encrypt Assistant Multi-Prime RSA) that could improve the performance of decryption and generation of signatures. The version will achieve high performance by rising modulus and private exponents.

#2 Research and Implementation of RSA Algorithm for Encryption and Decryption.:
Xin Zhou ,Department of Computer Science and Technology, Harbin University of Science and Technology, Harbin, China and Xiaofei Tang, Department of Software, Liaoning University of Science and Technology, Anshan, China

Conclusion:
As to protect confidential information from tampering, forgery, we need to secure it. And for it, the concept of encryption and decryption came into use. RSA is the first algorithm which can be used for both data encryption and digital signatures.. The key feature of public key cryptosystem is that the encryption and decryption is done with two different keys- public and private key.

#3: Design and Implementation of Client Server Based Application using Socket Programming
Rolou Lyn R. Maata, FCS, Gulf College, Sultanate of Oman, Ronald Cordova, FCS, Gulf College, Sultanate of Oman, Balaji Sudramurthy, FCS, Gulf College, Sultanate of Oman and Alrence Halibas, FCS, Gulf College, Sultanate of Oman

Conclusion: Socket programming is the best method in distributed computing (i.e. systems connected to same network) that can improve system performance. For OBS (Optel Billing System) application, Java Netbeans programming language is used as it covers a wide range of functions and classes.

#4: High Speed Implementation of RSA Algorithm with Modified Keys Exchange
Sami A. Nagar and Saad Alshamma, Faculty of Electronic Engineering, Sudan University of Science and Technology, Khartoum , Sudan

Conclusion: RSA algorithm is speeded up by generating keys offline and saving all key values in tables within database. Here, 4 security levels are proposed, each level with its own database. Before using the RSA algorithm, it must get an acknowledgment from RSA Handshake Database Protocol to create or update the identical gateway database.

#5: Implementation of Efficient Method of RSA Key –Pair Generation Algorithm
Yi Wu, Institute of Microelectronics, Tsinghua University, Beijing, China and Xingjun Wu, Institute of Microelectronics, Tsinghua University, Beijing, China

Conclusion:
The optimized algorithm was implemented to generate 1024 bits RSA key pairs based on smart card chip called THD8.

IV. RESULT

Here we can run several clients simultaneously.Where the server can encrypt all messages excluding the exit and joining message of the client. We also create a folder (i.e. public keys) where clients will store public keys in their own text file. If the client wants to leave the chat room, then the client must send the "Exit" message to the server. After that the client text file will be automatically deleted from the public keys folder. When the client successfully exits the chat room then existing clients will get the notification. If the server wants to leave the chatroom, then the server must send the "Exit" message to the server. After that connection will be lost and the client text file will be automatically deleted from the public keys folder. When the server successfully exits the chatroom then existing clients will get the notification

V. CONCLUSION

All chats interactions are handled in different client and server GUI. Also, it can work without network. Server acts as middleware between clients and shows the data encrypted.
Practices messaging. Shows message to check users that are newly connected and are online. Secured using RSA algorithm.

REFERENCES

[1] "Design and Implementation of an Improved RSA Algorithm" written by Yunfei Li, School of Information Science and Engineering, Yunnan University, Kunming, China and Quing Liu,Tong Li ,National Pilot School of Software, Yunnan University,Kunming,China.
[2] "Research and Implementation of RSA Algorithm for Encryption and Decryption" written by Xin Zhou ,Department of Computer Science and Technology, Harbin University of Science and Technology, Harbin, China and Xiaofei Tang, Department of Software, Liaoning University of Science and Technology, Anshan, China .
[3] "Design and Implementation of Client Server Based Application using Socket Programming" written By Rolou Lyn R. Maata, FCS, Gulf College, Sultanate of Oman, Ronald Cordova, FCS, Gulf College, Sultanate of Oman, Balaji Sudramurthy, FCS, Gulf College, Sultanate of Oman and Alrence Halibas, FCS, Gulf College, Sultanate of Oman.
[4] "High Speed Implementation of RSA Algorithm with Modified Keys Exchange" written by Sami A. Nagar and Saad Alshamma, Faculty of Electronic Engineering, Sudan University of Science and Technology, Khartoum , Sudan.
[5] "Implementation of Efficient Method of RSA Key –Pair Generation Algorithm" written By Yi Wu, Institute of Microelectronics, Tsinghua University, Beijing, China and Xingjun Wu, Institute of Microelectronics, Tsinghua University,Beijing,China.
[6]https://www.tutorialspoint.com/operating-systems-client-server-communication October 10, 2018 at 10.00am .
[7] https://www.javatpoint.com/socket-programming October 1,2016 at 2.30pm.
[8]https://www.gatevidyalay.com/transmission-control-protocol-tcp-header/ june 21, 2010 at 8.50pm.
[9]https://www.guru99.com/tcp-3-way-handshake.html January 2, june 12, 2015 at 10.30 am.
[10]https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/ june 15 , 2016 at 2.00 am.
[11] https://www.javatpoint.com/osi-model march 2, 2012 at 11.00pm
[12] https://secure.urkund.com/archive/download/74297140-282764-440023 june 20 , 2020 at 10.00 am