International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.7 March - April – 2023
DOI:10.46647/ijetms.2023.v07i02.095 ISSN: 2581-4621

Encrypted chat application using RSA Algorithm

Nuli Namassivaya[1],Sunkari Nithigna[2,] Sindhu Kovilala[3], MD Sibli Hussain[4]
[1]Associate Professor, Maturi Venkata Subba Rao (MVSR) Engineering College, *Hyderabad*
[2,3,4]Final year B.E.ECE Students, Maturi Venkata Subba Rao (MVSR) Engineering College, *Hyderabad*

***Abstract*—** In some ways, the potency and effectiveness of the knowledge systems rely upon its design and the way the knowledge area unit is transmitted among totally different parties. Similarly, a crucial side of computer code development is the security of the knowledge that flows through open communication channels. One of the foremost widespread designs is User/server design which creates the centralization of knowledge storage and process modification, and supply flexibility for applying authentication strategies and coding algorithms inside info systems. whereas the number of users increases, it needs to increase the authentication and coding levels as high as possible. users/servers could be a technology that enables the opening of an associate degree interactive session between the user's browser and also the server. during this study, we tend to use users/server design to accomplish secure messaging/chat between users while not the server having the ability to decode the message. During this manner, a Server Cryptography- based mostly Secure electronic messaging System mistreatment RSA (Rivest- Shamir Adelman), it is a widely used public-key cryptography and authentication system for encryption of digital electronic messaging transactions like email over the computer network, extranet, and net, to write in code and decipher messages is developed using Java Web Application.

Keywords—Cryptography, Rsa, Web application.

I.INTRODUCTION

The paper discusses circumstances under which such data can be used and how Message treats them. Many chats on a social/messaging platform have their terms and conditions about data. we can implement a secure chat application innovatively by using cryptography which provides reliability and confidentiality thus it can be effectively used by groups of people. even though achieving confidentiality requires a huge amount of cost we wanted to reduce the overall cost so we have chosen the RSA algorithm [1].

The paper aims to present a comprehensive study of security aspects in communication with RSA Algorithm. The article could open a discussion and highlight the problems of data storage and usage obtained from the communication and propose some standards to protect the user. Here we use the Cloud server to store chat in encryption using RSA. However, the safety elements in the chat space application area unit form certain all info from clients is shielded from hackers. The chat messages from users will simply remodel by professional hackers, while not an honest enough security element. The goal of this study is designed to accomplish the secure chat between users while not the server having the ability to decode. All the used coding processes supported the RSA algorithm.

RSA coding methodology is used to preserve the safety of the message stream.

Another way to reduce the length of encryption and decryption in the RSA cryptosystem is to use generic and private keys.

Allows for instant communications between users. Uses real-time chat over the network that can eliminate costly long-distance charges

II.PROPOSED WORK

For registering a new account, we need details such as name, email, and password. after registering email and password are checked by the server whether they are valid or not. after validation, these

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.7 March - April – 2023
DOI:10.46647/ijetms.2023.v07i02.095 ISSN: 2581-4621

details will be stored in the database. if the client makes a request these credentials will be validated from the database[2]

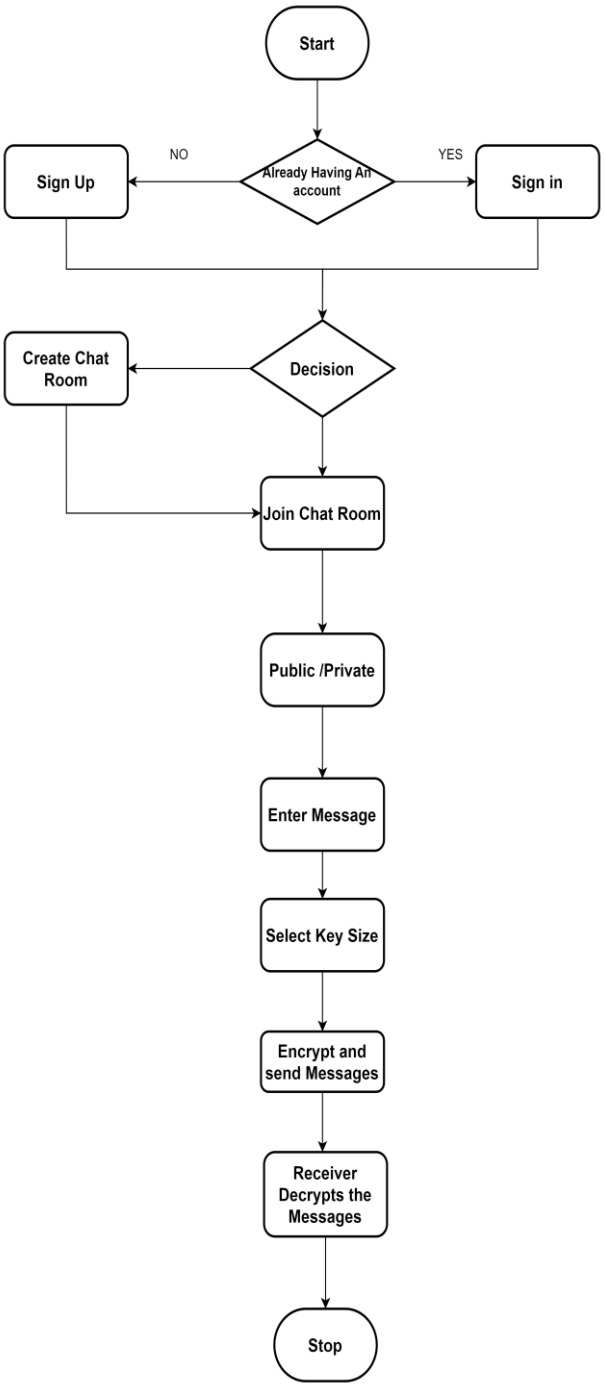

Figure 1: A Flow Chart illustrating the methodology.

1. Starting with the application if a user is new to the application, they are asked to register to get the privilege to access the application.
2. If the user has registered successfully, he can access the application by logging into the application. Once the user logs into the application he will be directed to the home page.
3. Here the user is given two options join a room and create a room. If the user is accessing the application for the first time a new room has to be created. The mode of the room may be public or private.
4. If the user selects to create a public chat room with immediate effect a room is created.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.7 March - April – 2023
DOI:10.46647/ijetms.2023.v07i02.095 ISSN: 2581-4621

5. But if the user selects Create private chat room user has to set a password for the room.
6. Now if the user wants to join a room, they can enter a
password to enter the corresponding chat room, or if it is the public user can directly enter the corresponding chat room.
7. User can now entirely message, click encrypt and send to other users in the chat room. Other users who want to read the text can decrypt and read the message.

A. Implementation of RSA Algorithm

The RSA algorithm was first used to implement the concept of public key cryptography and has been widely used because it is easier to understand and implement than other public key algorithms. Rivest Shamir Adleman's algorithm is the fastest and most efficient algorithm so far. RSA algorithm always works out with high accuracy, specificity, and security. and it also reduces the cost required for both encryption and decryption [3].

However, the RSA algorithm is computationally intensive with very large integer numbers. Strong primes are required for RSA security. Thus, the additional cost is indispensable for generating strong primes in RSA. The RSA key generation formula is defined as follows:

To find the keys, first let us select two large prime numbers which are p and q.

And now compute n=p*q

Choose a number e which is prime to the product (p-1) (q-1)

Where the e is the public exponent.

Compute an integer d from the quotient (ed-1)/(p-1)(q-1)

Where e is the private exponent. Even though we know the values publicly it becomes difficult to determine d from n and e. if p and q are very large. For encrypting the message M with the public key which creates the cipher text.

$$C=(M^{e}) \text{ MOD } n$$

The receiver decrypts the cipher text with the private key using $M=(C^{e}) \text{ MOD } n$

This is about the encryption and decryption process in the RSA algorithm.

B. Software Design

In designing the software following principles are followed:

1. Modularity and partitioning: software is designed such that, each system should consist of a hierarchy of modules and serve to partition into separate functions.
2. Coupling: modules should have little dependence on other modules of a system.
3. Cohesion: modules should carry out a single processing function.
4. Shared use: avoid duplication by allowing a single module to be called by others that need the function it provides.

C. Module Design

The major modules of the project are :

1. Admin

In this Module, Admin is used to log in, view users, view messages, and view users' requests for private keys.

2. User

In this Module, the user can view User Profile Add Room, View Room, Send Message, My Message, and View Messages

D. Input Design

Considering the requirements, and procedures to collect the necessary input data in the most efficiently designed. The input design has been done keeping in view that, the interaction of the user with the system is the most effective and simplified way. Also, the measures are taken for the following

- Controlling the amount of input
- Avoid unauthorized access to the classroom.
- Eliminating extra steps
- Keeping the process simple

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.7 March - April – 2023
DOI:10.46647/ijetms.2023.v07i02.095 ISSN: 2581-4621

At this stage, the input forms and screens are designed. nowadays chat applications are used tremendously because it connects a variable number of users. when we enter a message, for encryption and decryption a cipher key is generated randomly. and this cipher key will be used as the secret key. then this cipher text will be converted into plain text(i.e.) original message[4]

E. Output Design

All the screens of the system are designed to provide the user with easy operations more simply and efficiently, with the minimum keystrokes possible. Instructions and important information are emphasized on the screen. Almost every screen is provided with no error and important messages and option selection facilitates. Emphasis is given to speedy processing and speedy transaction between the screens. Each screen is assigned to make it as much user-friendly as possible by using interactive procedures. So, to say the user can operate the system without much help from the operating manual.

III. RESULTS

Figure: 2 Process followed while sending a message

As shown in the above fig, we have created a chatbot where both encryption and decryption take place. The plain text entered will be encrypted and converted into cipher text. Cipher text is in non-understandable form so to decrypt this message we need the private key. so that message becomes readable. Here both public keys and private keys are different .so we can maintain integrity and security for the system. After this process, we will be landing on the admin page, where we need to enter our name and password to log in. If we don't have an account, we need to sign in. so that these details will be stored in the database using MySQL. After logging in the user can view the person's name from whom they have received the message and the user can also see the kind of messages i.e., whether the messages are sent publicly or privately. If the message is public, the user can view the message without any key and if private, the user is required to decode the message using the private key. For decoding the message, the key is sent via E-Mail where we use a Simple mail transfer protocol (SMTP).

CONCLUSION

Demonstrating applicable Users/server applications could be a basic figure for planning, sending, and later ability. to prevent our data from undesirable hacking is the most important thing. because data is very sensitive it may contain our personal information or business information. so for providing a secure communication channel, we need to use encrypted messaging protocols which prevent data loss [5]. This paper highlights the utility needs for Users/server models and depicts configuration inquiries to be attended. A model re-enactment demonstrates dead an outsized range of

DOI:10.46647/ijetms.2023.v07i02.095 ISSN: 2581-4621

the conditions recorded, and its utilization was shown in an exceedingly few real and speculative illustrations. We tried with a user/server encrypted chat supported RSA by Web application. We've enforced the system in users/server design and a period network. We tend to believe that the system provides a high level of coding and additional flexibility in implementation.

REFERENCES

[1] T. Melo, A. Barros, M. Antunes, and L. Frazão, "An end-to-end cryptography based real-time chat," 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), Chaves, Portugal, 2021, pp. 1-6, doi: 10.23919/CISTI52073.2021.9476399

[2] Sabah, Noor & Kadhim, Jamal & Dhannoon, Ban N.. (2017). Developing an End-to-End Secure Chat Application. 17.

[3] Overview of Improvements and Modifications in RSA Algorithm", International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.1, Issue 7, page no. pp656-659, December-2014

[4] R. Pasumarty and R. P. K. N, "Secure Chatroom Application using Advanced Encryption Standard Algorithm," 2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON), Bengaluru, India, 2021, pp. 344-346, doi: 10.1109/CENTCON52345.2021.9688060.

[5] S. Nayak et al., "An application for end-to-end secure messaging service on Android supported device," 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2017, pp. 290-294, doi: 10.1109/IEMCON.2017.8117222.

Nuli Namassivaya, B.E. from Gulbarga University and M.Tech. from JNTU with Automation and Control Systems with University Topper. Presently he is working as Associate Professor at MVSR Engineering College, Hyderabad. He published 49 papers in International & National Journals & Conferences to his credit and 1 patent. He has 33 years of teaching experience. He is a Fellow member of IETE and a Life Member of CSI, IE(I), ISOI, BES, and ISTE. He served in various capacities in the above-mentioned Professional organizations. He obtained Rashtriya Gaurav Award from the India International Friendship Society, & the Best Citizens of India award in recognition of exceptional caliber and outstanding performance in a chosen area of activity by Best Citizen of India. His Biographical note is included in Asia/Pacific Who's Who. He was also awarded Bharat Ratna Rajiv Gandhi Gold Medal Award by Global Economic Progress & Research Association and Engineering Seva Ratna Award by ECI Foundation.

Nithigna Sunkari, B.E. from Maturi Venkata Subba Rao Engineering College(MVSR), Osmania University In Electronics and Communication Engineering stream has worked on Arduino based Smart Irrigation System.

Sindhu Kovilala, B.E. from Maturi Venkata Subba rao Engineering College(MVSR), Osmania University In Electronics and Communication Engineering stream has worked on automatic street lights using 555 timer circuits and LDR projects.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.7 March - April – 2023
DOI:10.46647/ijetms.2023.v07i02.095 ISSN: 2581-4621

MD Sibli Hussain, B.E. from Maturi Venkata Subba rao Engineering College(MVSR), Osmania University In Electronics and Communication Engineering stream has worked on Rain Sensing Automatic Car Wiper.