WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Secure Double Encryption Chatting Application

Madhuri Chelamasetti[1], Mallikharjuna Busani[2], Sairam Kukkala[3], Dr. P. Udayakumar[4]

[1,2,3]Department of CSE, [4]Professor

[1,2,3,4]Aditya Engineering College, Surampalem, A.P., India

ABSTRACT:

With the increasing amount of personal and sensitive information being shared online, it has become imperative to ensure the privacy and security of such information. Encryption is one of the most effective ways to achieve this. In this project, we propose the development of an encryption chatting application that will enable users to exchange messages in a secure and private manner. Our outcome will encrypt text on the device before sending a message. After user register into the application the user will receive a secret key from admin which is managed by application. After entering the key, the user can use the application and for every login the user receives a secret key by admin. For encryption and decryption Advanced Encryption standard (AES) is used.

INDEX TERMS: Chatting Application, NetBeans, Apache Tomcat Server, AES algorithm

INTRODUTION:

Chatting applications are software programs that allow users to communicate with each other via text, voice, and video messaging over the internet. These applications have become increasingly popular in recent years as more people have access to smartphones and other mobile devices that can connect to the internet. There are many different types of chatting applications available, including instant messaging apps, social media apps, and video conferencing apps. Some of the most popular chatting apps include WhatsApp, Facebook Messenger, WeChat, Skype, Zoom, and Slack. Chatting applications can be used for personal communication, such as keeping in touch with friends and family, or for professional purposes, such as collaborating with colleagues or conducting business meetings.

An encryption chatting application is a software program that enables users to send and receive messages that are protected with encryption algorithms. The purpose of encryption is to ensure that messages are only accessible to the intended recipient and cannot be intercepted by unauthorized third parties.

Encryption chatting applications typically use end-to-end encryption, which means that the message is encrypted on the sender's device and can only be decrypted by the intended recipient. This ensures that even if a hacker intercepts the message during transmission, they will not be able to read it. Encryption chatting applications are becoming increasingly popular as people become more concerned about their online privacy and security. These applications are often used by individuals who want to communicate sensitive information, such as journalists, activists, and business professionals.

AES (Advanced Encryption Standard) is a widely-used symmetric key encryption algorithm. It is a block cipher that operates on fixed-size blocks of 128 bits and uses keys of 128, 192, or 256 bits. AES was selected as the standard encryption algorithm by the US National Institute of Standards and Technology (NIST) in 2001, and it has since become the most commonly used encryption algorithm worldwide.

EXISTING SYSTEM

Data Encryption Standard Algorithm (DES) for Secure Data Transmission

Cryptography is a technique for secure data communication. Encryption is the process of encoding messages in such a way that only authorized parties can read it. DES works by

dividing the plaintext message into 64-bit blocks and then performing a series of 16 rounds of encryption on each block using a 56-bit secret key. Each round involves a combination of permutation and substitution operations that scramble the data in a complex way, making it difficult for an attacker to decipher the encrypted message without knowing the key.

The security of DES is based on the fact that the key space is extremely large, with 2^56 possible keys, making it computationally infeasible to crack the encryption by brute force.

Disadvantages

- Less secure
- Doesn't have specific length
- Key size (56 bits)
- Hardware implementations of DES are very quick.

PROPOSED SYSTEM

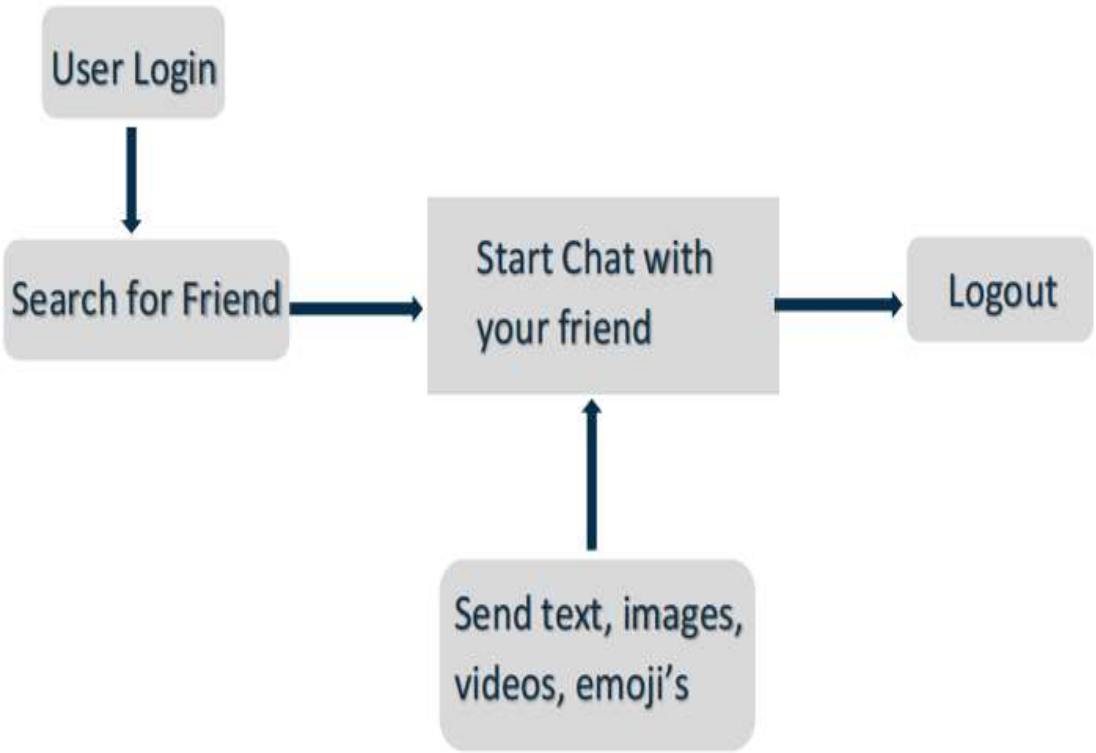
The system is an application that enables users to communicate with each other in a safe way and provides them with end-to-end security communication. This communication process is done through data encryption and submitted to the internet server in an encrypted format and then retrieved by certain queries and decrypted, then shown to the recipient user. The application consists of a set of interfaces design, which enable the user to perform the chat process with the rest of the users.

Advantages

- High Security: AES is a highly secure encryption algorithm that uses a 128-bit, 192-bit or 256-bit key to encrypt data. The encryption process is so complex that it is practically impossible to break the encryption and access the original data without the correct key.
- Wide Acceptance: AES is widely accepted and recognized as a standard encryption algorithm by governments, organizations, and industries around the world. This means that it is trusted by many and can be used for secure communication and data transfer.
- Fast Encryption and Decryption: AES encryption and decryption can be performed quickly and efficiently, making it suitable for use in many applications that require fast and secure data processing..

SYSTEM ARCHITECTURE

Fig 1



System Architecture

FLOW CHART

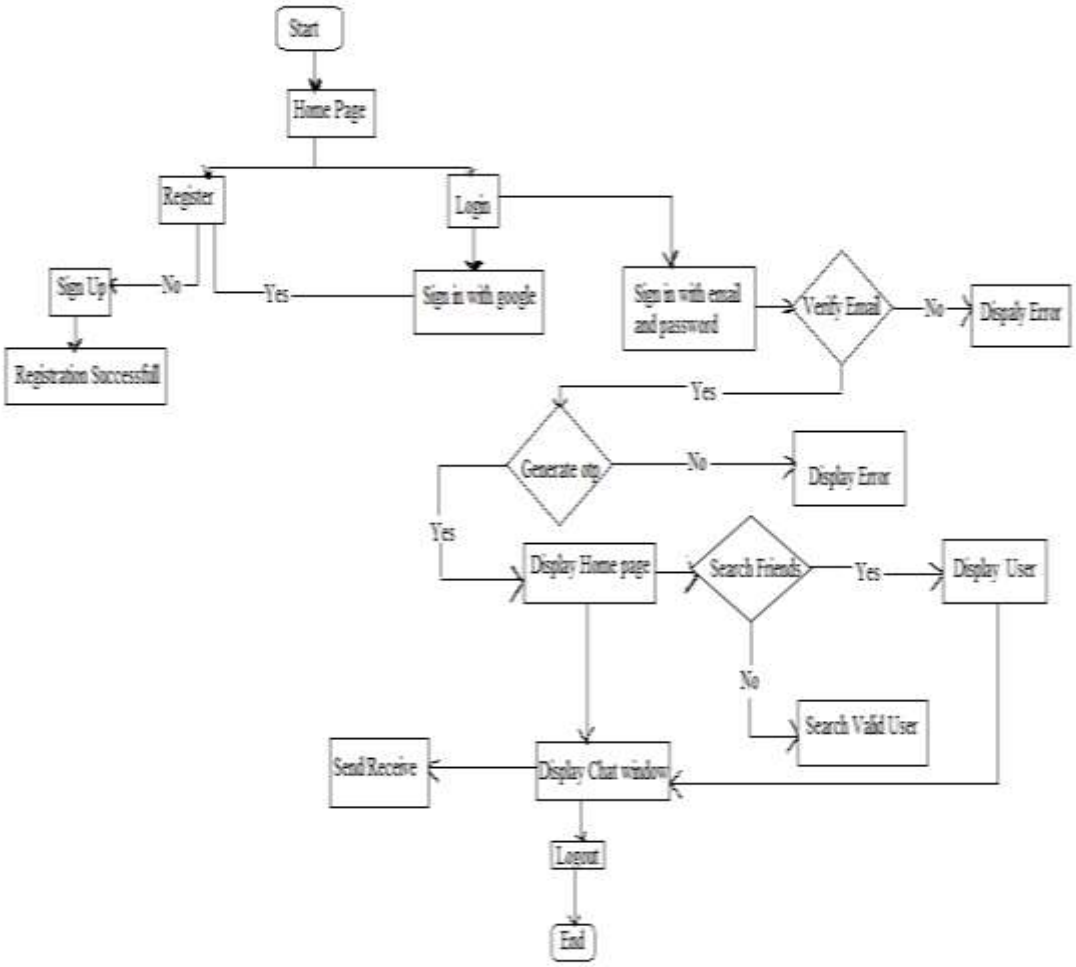


Fig 2 Flowchart

SYSTEM REQUIREMENTS

Hardware Requirement

- RAM - 4 GB and above
- Storage - 128 and above
- Code run - D drive

Software Requirement

Frontend : CSS, HTML,js,bootstrap,jsb

Backend : java and JDBC

Database : MySQL

Tools : NetBeans IDE,MySQL yog

Server : Apache Tom-Cat

Technology

Mern stack (for chatting application)

Algorithm

Advanced Encryption Standard (AES)

MODULE IMPLEMENTATION

The modules are as follows:

User Module

- Sign In
- Sign Up

Sign Up:

Sign up means "to register; to create an account". Sign Up allows the user to enter the personal information such as first name, Last name, Email, Password and Conform Password. After Sign Up it generates an OTP to registered mail. Entering of correct OTP gets registration successful.

Sign In:

A user sign-in module is a piece of software that allows users to authenticate themselves by providing a unique username and password combination or other forms of credentials, such as biometric data. This module is typically used in applications or websites that require user authentication to access specific resources or functionalities. Sign in allows user to sign with google or sign with email and password. After the user gets sign in successful the home page appears and user search it friends, if he enters valid user then it will display user details otherwise it will show enter valid user. When user hits enter to send a message, it will appear in the data base. The chats in the message box (decrypted) and data base(encrypted) are updated with new messages.

UML DIAGRAM

Class Diagram

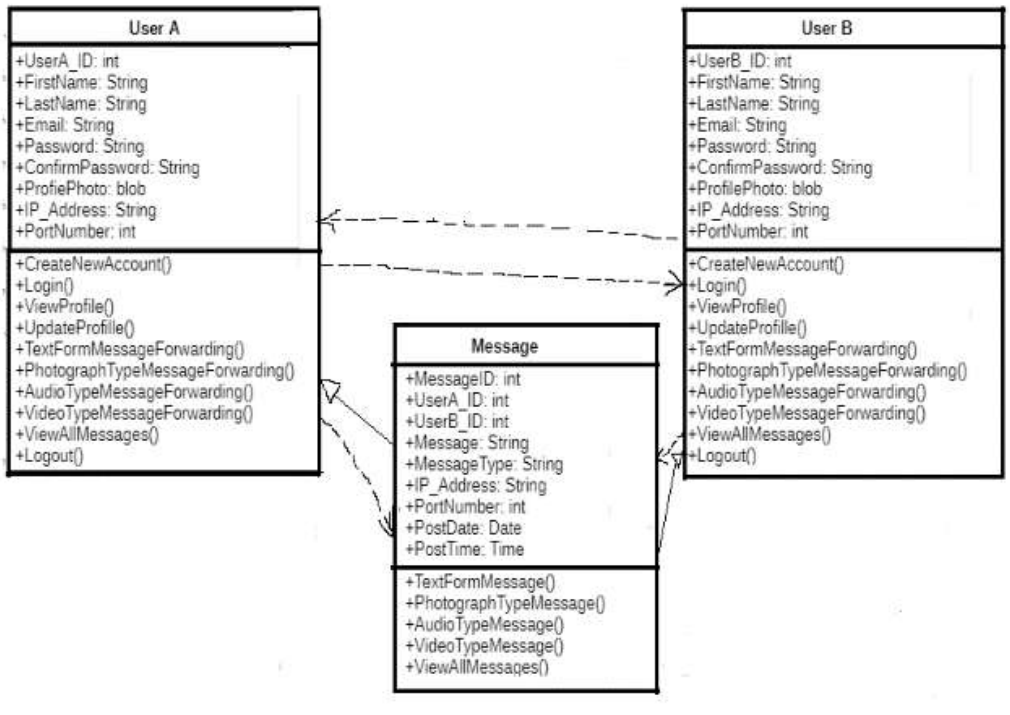


Fig 3 Class Diagram

ER Diagram

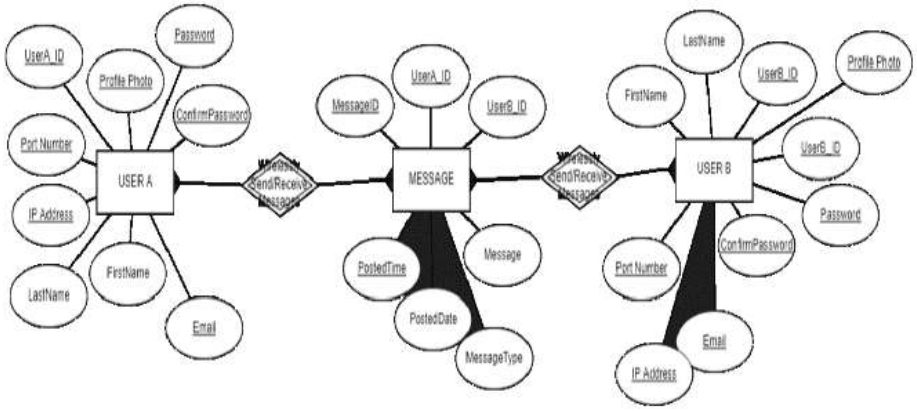


Fig 4 ER diagram

Use Case Diagram

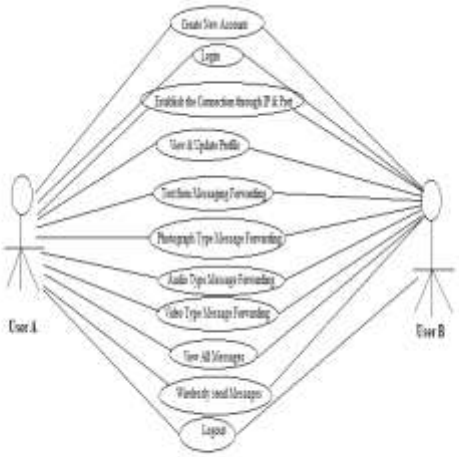


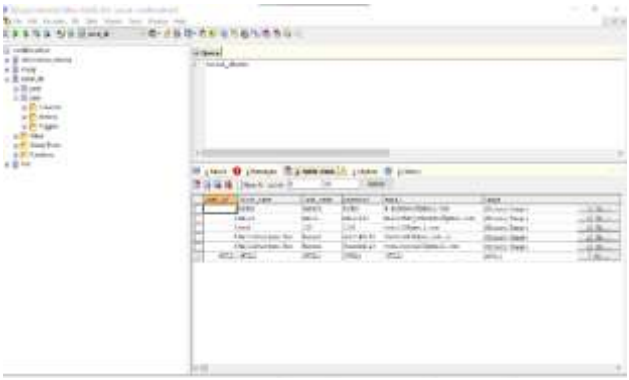
Fig 5 Use case Diagram

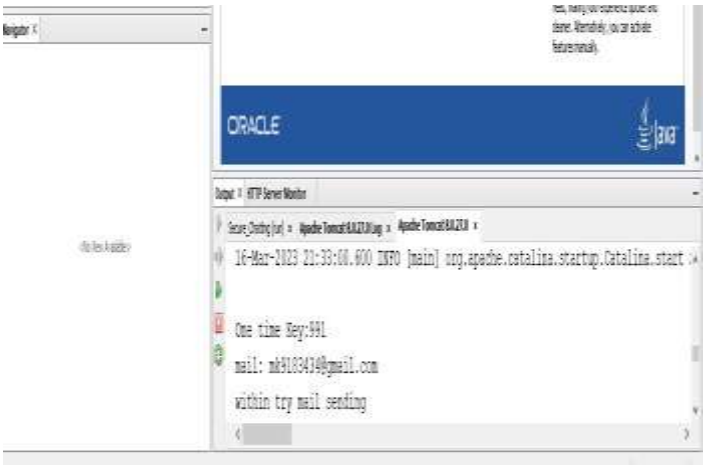
SCREENS

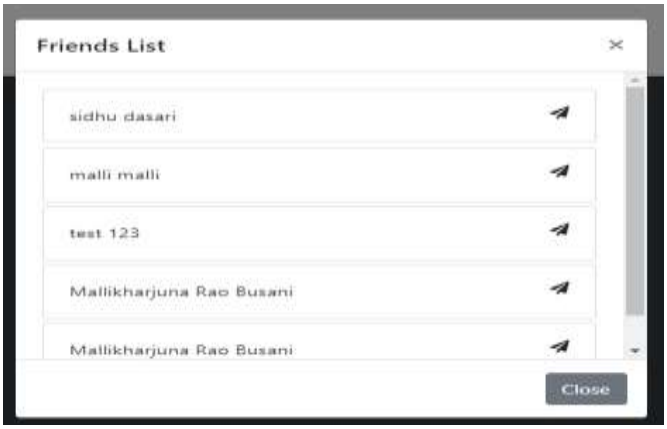

SIGN IN


SIGN UP


ENTER OTP SENT







RESULTS

Fig 6 End to End Encryption

CONCLUSION

In conclusion, an encryption chatting application using AES algorithm can provide a high level of security and privacy for its users. AES (Advanced Encryption Standard) is a widely recognized and highly secure encryption algorithm that can protect sensitive information from unauthorized access. By implementing AES encryption in a chatting application, messages exchanged between users can be securely encrypted and decrypted only by the intended recipients. This ensures that the messages cannot be intercepted or read by anyone else, including hackers or cybercriminals.

However, it is important to note that encryption alone may not guarantee complete security. Other measures such as secure password management, two-factor authentication, and regular software updates are also important for maintaining the security of the application.

FUTURE SCOPE

Our Chat application is made for connecting two individuals and allow them to chat personally share information we say that there's some limitations which we have to follow inorder to achieve, with this note we can say that our chat application will not allow users to create groups or adding participants into a single group and sending a mass message to all users at a time future enhancement be allowing users to create a group would and chat also making a video call chats.

REFERENCES

[1] Somen Nayak,Surajit Das,Saikat Das, Siddharth Sarker,Preyoshi Sarker,Aniket Dey "An Application for End to End Secure Messaging Service on Android Supported Device ",Conference on Vancouver, BC, Canada , 03 October 2017.

[2] Samira Prabhune,Sonal Sharma,"End-to-End Encryption for Chat App with Dynamic Encryption Key" Conference on Greater Noida, India, 18 December 2021.

[3] Sanket Anil Dambhare,"Design and Implementation of Encryption Tool using Advanced Encryption Standard (AES)" Conference on Tuticorin, India,18 March 2022.

[4] B. Bazeer Ahamed,Murugan Krishnamoorthy, "Fraction of Data in a Secure Client-Server Communication Method Using Key Exchange" Conference on Kochi, India, 15 September 2022.

[5] Rick Cents, Nhien-An Le-Khac,"Towards a New Approach to Identify WhatsApp Messages" Conference on Guangzhou, China, 09 February 2021.

[6] Nirmaljeet Kaur,Sukhman Sodhi "Data Encryption Standard Algorithm (DES) for Secure Data Transmission",International Conference on Advances in Emerging Technology , 2016.

[7] Mauli Bayu Segoro,"Implementation of Two Factor Authentication (2FA) and Hybrid Encryption to Reduce the Impact of Account Theft on Android-Based Instant Messaging (IM) Applications",Conference on Depok, Indonesia, 19 November 2020.

[8] Dijana Vukovic, DaniloGligoroski, ZoranDjuric, "CryptoCloak Protocol and the Prototype Application". 2015 IEEE Conference on Communications and Network Security (CNS), Sept. 2015

[9] Job J, Naresh V. K Chandrasekaran. "A modified secure version of the Telegram protocol", 2015 IEEE International Conference on Electronics,10-11 July 2015.

[10] Dr. Mohammed M. Alani ― "Improved DES Security", International Multi Conference On System, Signals and Devices, 2010.