International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

# Chit-Chat Box: A Real-Time Chat Application

Shashank Shekhar Chandigarh University Punjab, India
shashankshekhar7337@gmail.com

Ritesh Kumar Chandigarh University Punjab, India
ritesh00933@gmail.com

Aditya Upadhyay Chandigarh University Punjab, India
upadhyayaditya429@gmail.com

Himanshu Roy Chandigarh University Punjab, India
himanshuroy52hy@gmail.com

Daksh Jain Chandigarh University Punjab, India
dakshj287@gmail.com

Megha Sharma Assistant professor Chandigarh University Punjab, India

**Abstract:** In the digital era, online communications are a very important part of our lives. Chatting Applications, in particular, have become essential tools for those wishing to connect with other people over long distances. The software allows the user to share text. messages, images, and files in real time allow for smooth interaction. Existing Chat platforms often lack robust security features, adequate privacy settings, and efficient group management techniques—communication capabilities, raising red flags on data breaches and compromised user experiences.

This research paper suggests a new chit-chat application introduced and developed to address the deficiencies of current chat platforms by adding new features to enhance: privacy and group communication. In particular, our application will offer security-safe, reliable means of enabling users to communicate within a closed network-for instance, within corporate intranets. or a personal community. The app can be developed by using MERN stack, which is a common web full-stack development framework with MongoDB, Express.js, React.js, and Node.js to provide a robust and scalable solution.

The main features of Chit Chat Box include:

• **Enhanced security:** Chit Chat Box respects end-to-end encryption, which indicates that messages are secure from any eavesdropping. No data or user credentials, and chatting history, are securely stored in MongoDB, ensuring its privacy and confidentiality of user information.

• **Group Communication Features:** It lets users create group conversations. and share messages with multiple recipients at once. This feature allows for ease of collaboration in communication, keeping users in touch with their colleagues friends or family members.

• **No Direct Messaging:** Chit Chat Box doesn't allow users to directly message other users without having established a connection through a mutual group or community. This measure helps prevent unsolicited messages and makes for a more disciplined and respectful communication environment.

• **Screenshot Protection:** Chit Chat Box is designed to prevent users using state-of-the-art technology from taking screenshots of conversations. It protects sensitive information from screenshots and makes sure that, private talks stay private.

This paper will cover the technical details of the Chit Chat Box application by describing its design principles, implementation methodology, and security measures. Let's talk about how this involves challenges in the developing process and highlights major innovations that differentiate the Chit Chat Box from other chat applications.

**Keywords:** secure chat application, user privacy, group communication, HTML, CSS, JavaScript- Real-time Communication.

## I. Introduction

The internet nowadays is ubiquitous and has revolutionized the way we communicate and

collaborate. Online chat platforms are now an integral life tool of everybody who wants with others over a long distance. The chatting applications allow the users to share text messages, images and files sent in real-time to facilitate seamless interactions. Ease and the efficiency in them has made chat applications ubiquitous, and their implementation is now used across vast contexts, from personal communication to business collaboration to even education. [1, 2]

However, most existing chat platforms have several limitations that can compromise user Safety and Security. Some of such are:

• **No End-to-End Encryption:** The majority of chat applications do not introduce end-to-end Encryption which means end encryption, whereby messages can be intercepted by third parties and read. This, in itself, could be a major issue for the users in terms of their data security. who is sharing sensitive information? [3]

Ex: WhatsApp, a widely used chat messenger over TLS, used only earlier. (Transport Layer Security) to secure the channel, which in turn meant that the all messages exchanged was available to the service provider. This practice raised concerns of privacy for users who believed their conversations were private and CONFIDENTIAL [1]

• **Limited Privacy Setting:** Most of the chat applications have limited privacy settings. This makes it difficult for the users to control which information from their messages other people can see. is shared, which can eventually lead to the breach of privacy and unauthorized disclosure of sensitive information. information. [4]

Ex: Some chat applications do not allow their users to control who may see their online status or the ability of the feature to notify the contacts in case they are sending a message. Such lack of control may attract unwanted attention and even Harassment. [2]

**Ineffective Group Communication Features:** Most of the chat applications lack powerful group communication features that made it difficult to organize and communicate with several people simultaneously. This could be a huge challenge for Organizations and teams that use chat apps to collaborate:

Ex: A number of the chat applications don't support group chats, or It easily allowed the user to add or delete members from a group. Lack of could weigh heavily on teams requiring the coordination of activities or Sharing information [3]

Considering these limitations, this paper will propose a new use of the chat application, entitled "Chatterbox – a real-time chat application " designed especially to securely and reliably allow the users to speak in a private network, in an intranet of an organization, or even a closed community.

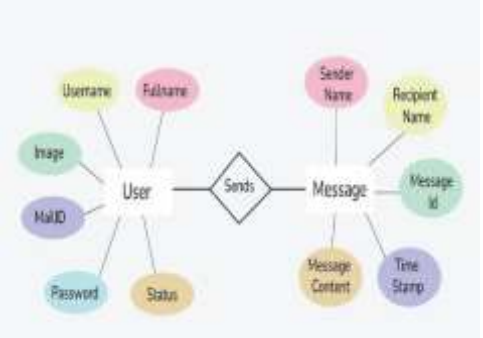
The app is designed in HTML, CSS, and JavaScript with advanced security. measurements and innovative design principles to make it robust and user-friendly.

**Why is Chit Chat Box important?**

Chit Chat Box addresses the pressing need for a secure and reliable communication platform in the highly integrated world of today. The commitment to distinctive application features users' privacy is a hallmark of this application, making it suitable for organizations and individuals who are looking platform for exchanging sensitive information and collaborating effectively.

The app's innovative approach to security, group communication, and privacy assures users can be confident that they can communicate in a safe closed network and, their conversations are securely protected from potential illegitimate access and eavesdropping. The development of the Chit Chat Box is a huge step toward developing a more secure reliable and easy-to-

use chat functionality will create a more secure and safe online communication setting.




## II. Literature Review

Communication has been redefined with the integrated use of chat applications in the digital age. Users can exchange text messages, images, and files within these platforms in real-time, and this enables seamless cross-geographical interactions. However, existing chat platforms often struggle with addressing the very concerns related to security, privacy, and user experience. This literature review searches for the challenges imposed on these limitations and it responds to the need for secure and featured chat applications.

**1. Security-based issues in today's chat applications:**

Security for many chat applications is incomplete, as users are highly vulnerable to potential vulnerabilities. The main concern is the lack of end-to-end encryption, which intercepts messages, which are read by service providers, among other third parties. What this means is that this practice raises serious privacy concerns because the users expect the conversations to remain private classified.

• **No End-To-End Encryption:** Famous chat apps like WhatsApp previously

used only TLS, or Transport Layer Security, to secure the channel—meaning that the service provider had access to all messages exchanged. The practice made privacy concerns worries for users who wanted their conversations to be kept confidential. [1]Data Storage and Access: Most chat applications store messages and any other user data. contact details and geolocation information in centralized servers, a practice that has raised raises concerns about a breach of information and unauthorized access because this Data is under the provider's control. [2]

**2. Poor Privacy for Already Existing Chatting Applications:**

Another major problem faced by chat applications is the absence of strong privacy settings. Since many applications do not give users adequate control over who can see their messages what information shared, and how their online appearance is presented. This loss of control can take to privacy infringements and unwanted attention.

• **Online status control:** Not all chat applications give their users control over whom can tell when they are online, or to disable notifications for contacts that they are text a message. This lack of control could result in even negative attention and even Harassment. [3]

• **Group Chat Privacy:** Most chat apps have next to no settings for ensuring chats, which creates difficulty for users to manage the level of privacy and control who can join or leave the group. The inability to police can lead to inadvertent disclosure of private data. [4]

**3. Anti-productive Features of Group Communication:**

Many chat applications lack robust group communication features, making it difficult for users to organize and communicate with multiple people simultaneously. This limitation can be a major challenge to organizations and teams that depend on chat apps for communication.

• Limited group chat capabilities because not all of these chatting applications support the creation of group conversations allows users to add or remove members from the group easily. this lack of functionality can be cumbersome for

teams that need to coordinate and share information or activities. [5]

• Lack of collaboration tools: Most of the chat applications lack features that facilitate collaboration, in ways such as file-sharing, task management, and document editing. This lack Most of the functionality makes collaboration by users difficult. [6]

**4. Growing needs for secure fully-fledged chat applications**

**Limitations of existing chat apps pinpoint the need for security with feature-rich:**

Platforms that relieve users of their concerns about privacy, security, and collaboration. Secure chat applications should ensure end-to-end encryption, assurance of strong privacy settings, and offer effective group communication features. Additionally, such applications need to be user-friendly.

**5. Current Works on Research and Development:**

Besides, active researchers and developers are trying to surpass the existing limitations of chat applications. Certain key areas of investigation include:

• **Designing more secure encryption techniques:** New designs are under study. Encryption algorithms and protocols to provide further security and resistance to attacks. [7]

• **Enhancing Privacy Settings:** Developers are working towards more stringent privacy settings in chat applications that grant them the power over who can view their messages. Information is given out, on how their online presence is portrayed. [8]

• **Group features enhancing communication:** The developers are adding more groups Besides communication features, it provides file-sharing and task-management chatting applications. document editing. Besides, they work on new features for improving the user experience forgroup users This makes chats work more effectively and be friendly.

## I. Design and Architecture

The architecture of Chit Chat Box will be such that it provides a secure and reliable platform for communication within a closed network. This application follows the client-server architecture; the client application shall run on the web browser of the user, while the server application shall run on a server dedicated to the application.

### 3.1. Client-Side Application

The client-side application will be designed in such a way that it provides a friendly interfacing to its users with the help of HTML, CSS, and JavaScript. The application would include, on the client side:

• **Login/Registration**: Users can log in using their existing account credentials or create new accounts.

• **Contact List:** It lists down all the contacts of the user that would get populated automatically from the server.

• **Group Chat:** A user can create a group chat and share messages with multiple receivers.

• **Message Display:** This application will display all messages in the order they have been received, and each message is time-stamped to give context.

• **Input Box:** One can input a message and then click send for other users to see.

• **Notification System:** A new message, friend request, etc., would be notified by the application.

### 3.2. Server-Side Application

The Node.js-Express.js server-side application is concerned with user authentication, persists any data that should be permanently stored, and allows clients to establish real-time communication amongst themselves. Subsequently, the server-side application comprises the following components:

• **Authentication Server:** This handles user login and registration requests, confirms user credentials, and keeps user information.

• **Message Server:** This routes messages amongst the clients, storing the chat history in the database and updating the clients in real time.

• **Database:** The application uses a relational database, such as MySQL or PostgreSQL, to keep the users' data, including their contact information, chat history, and other relevant information.


### 3.3. Security and Privacy

The following describes how security and privacy are kept at the Chit Chat Box:

• **End-to-end Encryption:** All messages exchanged by the clients are end-to-end encrypted using XSalsa20 cipher algorithm. [4]. Implementation The encryption process will be performed completely client-side using a client- side library in JavaScript like CryptoJS. When a user sends a message to someone, the client encrypts the message with the recipient's public key. The encrypted message is sent to the server,

which sends it to the targeted recipient. The client of the recipient decrypts the message using his/her private key. The disadvantage of this is that only the recipient can read the message because the server doesn't have the key for decryption. Secure Session keys Application uses ECDH- Elliptic Curve Diffie-Hellman, which establishes the secure session keys between the clients."5 These keys are never stored on the server and are known only to the communicating parties-issues impossible for third parties to access the conversations.

Implementation: ECDH is an interoperable key agreement protocol whereby two parties derive a shared secret key over an insecure channel. This symmetric shared secret key is then used to encrypt and decrypt messages exchanged between the parties.

**Benefits:** ECDH is a secure key exchange protocol that is resistant to man-in-the-middle attacks.

• **Secure Password Storage:** Passwords stored in the database are hashed using a strong hashing algorithm like encrypt. [6] This makes the password-cracking job

difficult for hackers even if the database gets compromised.

**Implementation:** When a user creates an account, their password is first hashed with bcrypt and then stored within the database. If a user tries to log in, their password is hashed again and compared to the stored hash. If they match, then the user is authenticated.

**Benefits:** Bcrypt is a hashing algorithm that is computationally expensive to run.

Difficult for even brute-force attacks to crack passwords.

• **Data Protection:** The application secures the data stored in the database by using AES- 256+SHA2 encryption. [7] This would guarantee that only the authorized users could access the sensitive information.

**Implementation:** The data to be stored in the database, which contains user credentials and history of chats is encrypted by AES- 256+SHA2 before storing. The Application uses one encryption key per user for added security of data. NO Benefits: AES-256+SHA2 is a strong encryption algorithm that finds widespread use in securing sensitive data, such as financial information and personal records.

### Implementation Details

Chit Chat Box is implemented using the following technologies and tools:

• **HTML:** It is used to provide structure to the content of web pages by defining the elements such as headings, paragraphs, lists, and images.

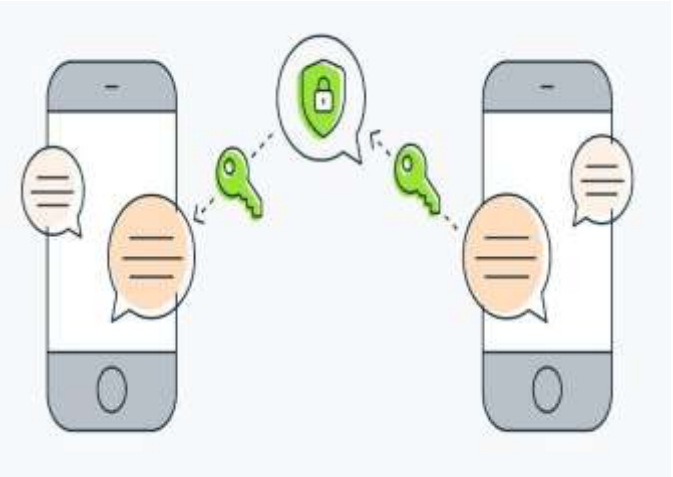
• **CSS:** It is used to style the visual presentation of web pages by defining elements such as colours, fonts, and layout.

• **JavaScript:** It allows the web pages to be interactive and dynamic. It runs user inputs, manipulates the DOM, and sends and receives data from the server.

• **Node.js:** The application does use Node.js in building the server-side application and also handles the authentication for users, properly storing data.

• **Express.js:** Express.js is fundamentally a web application framework for Node.js that simplifies code implementation REST APIs development used for interaction between client and server. [9]

• **Relational Database:** The relational database of the application relational database like MySQL or PostgreSQL stores the data regarding the users, information about their contacts, chat history, and other information regarding the users.



### New Features

Chit Chat Box offers a range of new features involving security, privacy, and group communication:

• **Multiple Message Forwarding:** This tool allows users to forward messages to several recipients at once. This feature allows users to share information, announcements, or updates with users.
**Implementation:** When the user wants to forward the message, the application lists of their contacts. The user can select multiple contacts from the list and the message will be forwarded to each selected contact.

• **No Security:** For the message not to be accessed by an unauthorised user, the message is first encrypted using the XSalsa20 algorithm and using the session key of the recipient before it is forwarded.

• **No Direct Messaging:** Users are not allowed to directly message other users by taking their contact number from any common group or community. This measure prevents unsolicited messages and spam, thus improving the user experience.
**Implementation:** The application does not allow access to contact information of other users directly. The only way to start communicating with another user is through a common group or community.
**Benefits:** This feature assists in creating a more controlled and respectful It helps to create a very friendly environment for communication and

protects users from information they don't want to receive.

• **Protection of Screenshots:** Users cannot capture the screenshot of conversations. This feature protects sensitive information and helps keep the privacy of conversations. **Implementation:** The application uses both browser-level and server-level methods to prevent a user from capturing screenshots of conversations. Browser-level techniques

involve disabling the right-click menu and utilizing JavaScript to detect and block attempts at taking screenshots. Server-level Some of them are the watermarking messages with timestamps and user information. Security: This feature enhances the security and privacy of applications by preventing unauthorized sharing of sensitive information.

## Conclusion

Chit Chat Box is a secure and reliable chat application that solves the deficiencies in the current Chat platforms. This chat application ensures the security and privacy of the users by introducing end-to-end encryption in messages, protection in session keys, and data protection policies. The features introduced in the application for Group communication like the message forwarding feature to multiple users and the prohibition on direct messaging to one user have further enhanced the user experience.

This would leave the communication environment much neater and polite. In this regard, Chit-Chat Box's development marks a very significant step towards making this chat platform secure, reliable, and user-friendly. Due to its novelty features, commitment to privacy, and security, this application stands out as ideal for both organizations and individuals with needs for strong and reliable communications solutions. Further development of Chatter Box.The Chat Box will focus on further enabling capability and refining the user experience.

## References

**1.** "WhatsApp Encryption Overview." [Online]. Available: https://www.viber.com/security-overview/.
**2.** "Telegram F.A.Q." [Online]. Available: https://telegram.org/faq.
**3.** "Active Sessions and Two-Step Verification." [Online]. Available: https://telegram.org/blog/sessions- and-2-step-verification.
**4.** "XSalsa20." [Online]. Available: https://en.wikipedia.org/wiki/XSalsa2 0.
**5.** "Elliptic Curve Diffie-Hellman (ECDH)." [Online]. Available: https://en.wikipedia.org/wiki/Elliptic _Curve_Diffie%E2%80%93Hellman.
**6.** "Bcrypt." [Online]. Available: https://en.wikipedia.org/wiki/Bcrypt.
**7.** "AES-256+SHA2." [Online]. Available: https://en.wikipedia.org/wiki/Advanc ed_Encryption_Standard.
**8.** "Node.js." [Online]. Available: https://nodejs.org/en/.
**9.** "Express.js." [Online]. Available: https://expressjs.com/.
**10.** "MySQL." [Online]. Available: https://www.mysql.com/.
**11.** "PostgreSQL." [Online]. Available: https://www.postgresql.org/.
**12.** "CryptoJS." [Online]. Available: https://cryptojs.org/.
**13.** "NordVPN" [Online] Available: https://nordvpn.com/blog/most-secure- messaging-app/
**14.** "Avast" [Online] Available: https://www.avast.com/c-most-secure- messaging-apps
**15.** "Geeksforgeeks" [Online] Available: https://www.geeksforgeeks.org/online-chat- application-project-in-software-development/