Chatify: A Secure End-to-End Encrypted Real-Time Chat Application

Akshat Kumar Srivastavaa
Department of Computer Science and Engineering
Galgotias University
Uttar Pradesh, India
akshat.22scse1010209@galgotiasuniversity.edu.in

Vaibhav Mishra
Department of Computer Science and Engineering
Galgotias University
Uttar Pradesh, India
vaibhav.22scse1010779@galgotiasuniversity.edu.in

JN Singh
Department of Computer Science and Engineering
Galgotias University
Uttar Pradesh, India
drjnsingh@galgotiasuniversity.edu.in

***Abstract*—Real-time chat applications have become an integral requirement within technology-based communication systems. However, concerns regarding data security, hacking, and centralized message storage have increased significantly. Most existing chat applications rely on centralized servers, making them vulnerable to security breaches. To address these issues, this paper proposes Chatify, a secure real-time chat application using end-to-end encryption.**

The system is developed using the MERN stack and supports real-time messaging through WebSocket communication with Socket.io. Messages are encrypted at the sender's side and decrypted only at the receiver's side, ensuring that even the server cannot access message content. This work demonstrates how modern cryptographic techniques combined with web technologies can enable private, secure, and efficient real-time communication.

***Index Terms*—Real-Time Communication, End-to-End Encryption, Secure Chat Application, WebSocket, Socket.io, Web Security, MERN Stack**

I. Introduction

Real-time digital communication is an integral part of everyday living and sustains not only interpersonal communication but also collaboration and coordination. It wasn't too long ago that the use of web messaging applications began a rampant growth because of the potential benefit of allowing increased collaboration through messaging and sharing sensitive information through chat messaging tools. However, with the increase in using such tools, concerns about security and access have become very prominent. Most conventional chatting apps use the centrally controlled communication pattern; hence, messages are processed on servers through unencrypted or partly encrypted forms. In these systems, the users' data can easily be exposed to various threats related to data breaches, surveillance, and insider attacks. Also, in transport-layer-encrypted systems where users' data is encrypted on one end, privacy risk ensues. Thus, confidentiality maintenance for messages has emerged as an increasingly important challenge for modern RT communication systems.

E2EE has proven to be a useful tool in overcoming these challenges by allowing only the parties involved in the communication to read the message. On a closed E2EE network, a message is encrypted on the sending device, allowing it to be readable only to its intended recipient, which means third-party entities like servers are not able to read it. But incorporating E2EE in real-time online chatting technologies poses a number of challenges.

In this context, Chatify is an example of a secure real-time messaging application that combines cryptography with web technologies. The proposed work is based on the use of the MERN technology stack and implements messaging via WebSockets with Socket.io. The aim of Chatify is to combine strong cryptography with modular software construction. This is achieved by ensuring proper authentication with secure messages transmitted over strong cryptography and ensuring reliable real-time messaging.

This project targets the design and implementation of a secure end-to-end encrypted messaging application for chat that focuses on privacy and at the same time offers expected performance and usability associated with modern messaging services. Through incorporation of modern web technologies and encryption techniques, Chatify highlights that real-time digital communication can be both functional and secure.

II. Literature Review

With the ever-increasing use of internet communication platforms available online today, there arises a greater need for live online chat applications as a means of online communication. There have been different researches conducted online concerning the design, implementation, or development of online messaging systems using different technologies such as WebSocket, Node.js, and NoSQL databases for achieving the feasibility of low latency and scalability for communication. Although such systems are very efficient for message transmission purposes, the aspect of security and privacy comes next.

Traditionally, the first messaging applications were primarily designed to serve their functionalities and performance. This was made possible by using the server for message handling and storage. Research shows that the centrally managed architecture used in servers makes the messages prone to risks such as hacking and monitoring by servers. In addition to this, messages in servers are intercepted even in clear text form despite using transport layer encryption such as HTTPS and TLS.

Although these messaging services have disadvantages, there have been researchers who have suggested the use of certain techniques from the cryptography domain for messaging services. End-to-end encryption has become a widely adopted solution for ensuring that no one except the individuals who are part of communication can access their massages. Different research works carried out regarding secure messaging services have demonstrated that E2EE can be a successful solution for eliminating leakage risks with respect to data leakage and prevention from access by any third party, such as messaging service providers. Some messaging services might have difficult conditions for applying E2EE.

The ongoing research work has also explored the idea of integrating WebSocket Communication with encryption methods for supporting the purpose of secured messaging. The application of libraries such as Socket.io for supporting bidirectional communications provides a competent means of carrying out the communications effectively with higher levels of performance when compared to the HTTP polling method. After applying the encryption methods with these libraries, secured communications can be carried out efficiently.

Despite the improvements developed in the above researches, most of the current research works have been focusing on the real-time communication performance or the cryptographic security respectively. Very few researches have been conducted on the secure web application based on the end-to-end encryption with the web application framework.

Despite all those advances, there are many studies either concentrating on real-time communication performance or cryptographic security. It seems there is no work done for the integration of end-to-end encryption into a web-based real-time chatting system. This provides clear implications for a need to exist for a solution for the combination of those concepts. The proposed chat app, named Chatify, aims to address the inadequacies listed above by combining the benefits of end-to-end encryption with real-time communication functionality using the MERN stack and WebSockets. The convergence of strong encryption methods and advanced web development tools, as offered by the Chatify solution, is a significant move forward to develop real-time chat solutions which are secure, privacy-focused, and efficient.

The approach emphasizes the design of the system, secure communication methods, and efficiency in the execution process rather than focusing on analysis. The technique integrates the development of the system with methodologies for security and effective communication.

III. Research Methodology

In the context of the Chatify system, it can be identified that the methodology for conducting the research work involves a design-focused and implementation-based method whereby the intended aim would be the creation of a secured communication platform with real-time support and end-to-end connectivity.

The approach proposed here relies on the design of the system, the security of communications, and efficiency. The approach proposed here incorporates the design of the system along with the existing knowledge concerning security and communications.

This will include coming up with functional and security requirements, designing a scalable system design utilizing Web technologies, and designing encryption approaches to safeguard the confidentiality of messages. This design will be evaluated considering the analysis of reliability of secure messages and the response of the developed system. This design will guarantee that applying the proposed security will not enhance complicating the usability of the developed system.

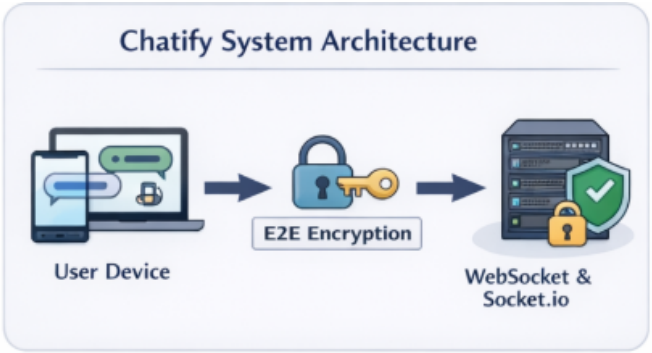

Fig. 1. Performance and Security Analysis of the Chatify System

IV. Data Collection

The data collection for the “Chatify system” is essentially qualitative in nature, as it assesses the behavior of secure real-time communications rather than other performance aspects. The observation is made on the basis of interaction in the system that takes place during the real-time exchange of messages, the authentication of the user, and the transmission of encrypted messages to the other user.

In this assessment, the system functionality with regard to the secure transmission of messages, the storage of the messages encrypted, requests for authentications, and the real-time communication through the use of WebSockets is also analyzed. As discussed earlier, the system functionality with regard to the reliable transport of messages, the integrity of the encrypted messages, and the responsiveness of the system to the use cases will be essential in determining the success of the implemented mechanisms in securing the confidentiality of the messages.

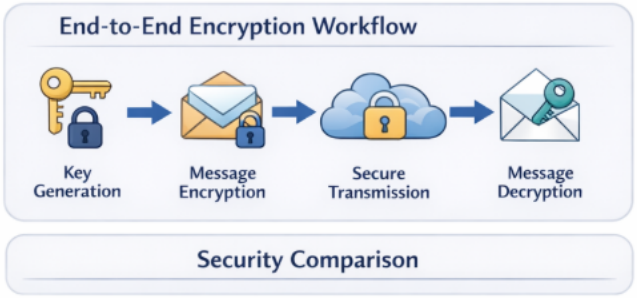

Fig. 2. Data collection overview depicting encrypted message transmission events, user interaction patterns, and secure communication behavior in the Chatify system

V. Data Analysis

The data gathered is used to analyze and validate the capability of the Chatify mechanism in protecting and granting reliable real-time communications. Data processing is conducted by observing the sending of encrypted messages and the effectiveness of the authentication mechanism of the Chatify system in a live chat setup. Great analysis is performed based on whether the sent messages are truly secured, meaning that data confidentiality is truly maintained during transmission and storage, and unauthorized parties-even the server-do not have access to plaintexts.

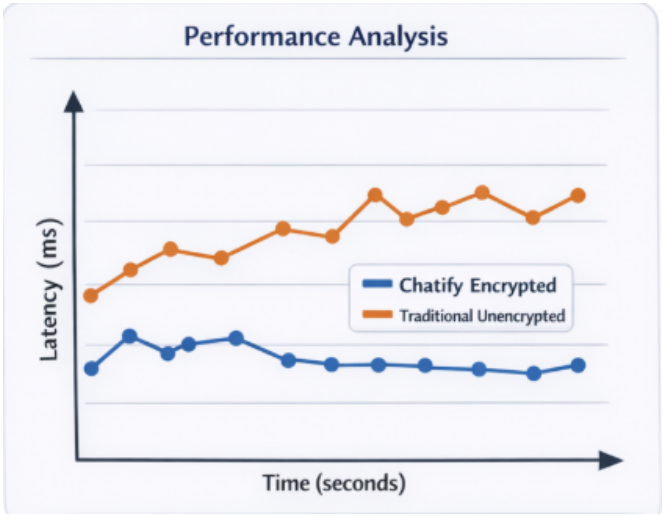

Fig. 3. Data analysis of encrypted message transmission and performance behavior in the Chatify system

Additionally, the testing that will be conducted in the analysis will revise reliability of message delivery, integrity of encryption, and stability of WebSocket connections for a real-world usage scenario. It also takes into consideration various usability aspects: response time, smooth messaging, and overall user experience, ensuring the integration of end-to-end encryption does not adversely affect system performance while communicating securely.

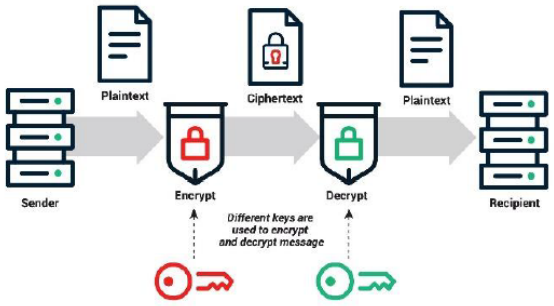

Fig. 4. End-to-End Encryption process illustrating secure message transmission from sender to recipient using encryption and decryption keys.

VI. Results and Discussion

Based on the analysis outcome, it is clear that the Chatify system is capable of offering a safe and reliable means of real-time communication through the successful application of encryption. During the real-time communication process, the messages passed through without any delays while being encrypted until they reached storage. This is a crucial component because it ensures that messages are not intercepted through server and/or unauthorized sources.

The results also indicate that the concept and implementation of Chatify are successful in achieving the secure end-to-end encryption for the real-time chat functionality. The encryption of the message is done at the sender's side and can only be decoded at the receiver's side, thus ensuring the success in maintaining data confidentiality.

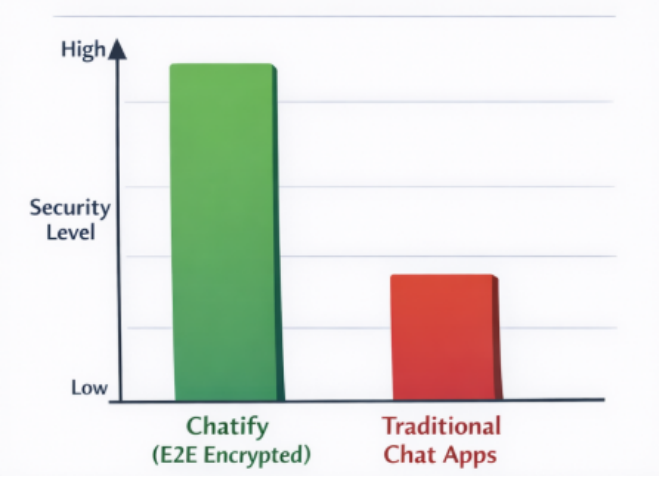

Fig. 5. Result Based On Experiment

The addition of communications using WebSockets will ensure that there is effective passing of messages; hence it is fit for real-time communications. The authentication methods concerning session retrieval will ensure that only authenticated users are able to participate in a communication session. In general, the findings have confirmed beyond doubt the need for a balance related to the securities of the performance and

functionality of the system for the efficiency of the proposed system, Chatify, as a real-time chat system.

VII. Conclusion and Future Scope

Chatify- An end-to-end encrypted real-time chatting application for hassle-free and secured digital communications. In the proposed model, encryption performed on the sender's side and decryption performed exclusively at the receiving side prevents the leakage of message contents from unauthenticated access, such as the server's access. The addition of web technologies to the proposed model provides hassle-free real-time communications with secured privacy.

This implies that the Chatify has been successful in incorporating the aspects of security, performance, and usability within the single platform of communication. Since the communication system implemented is based on the use of WebSockets, this will contribute to the support of the communication system related to the low latency messages. Additionally, the system will be improved with the increased reliability associated with the whole system.

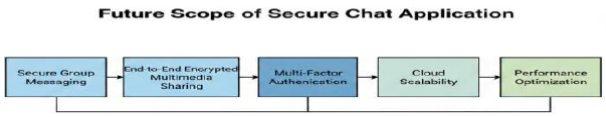

Fig. 6. Vaibhav-7: Future scope of the proposed secure chat application highlighting secure group messaging, encrypted multimedia sharing, multi-factor authentication, cloud scalability, and performance optimization

That will involve the future work that will encompass the incorporation of efficient techniques for the key handling process, the incorporation of the messaging system within the groups securely, and the end-to-end image encryption. Other variables that will be part of the improvement will encompass the multi-factor authentication process as well as the scalability aspect.

Acknowledgment

The authors are pleased in acknowledging the fruitful guidance and support given by Dr. J. N. Singh during the execution of this research work. The authors are thankful to all the faculty members of the department of computer science and engineering of Galgotias University for extending their support and encouragement. Their thankfulness goes to Galgotias University for having made an appropriate environment to finally accomplish the submitted research work. The authors want to extend their gratitude to the editors of this journal for having published this work.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[2] A. Green and M. Smith, "The Cryptopals Crypto Challenges," Cryptopals Crypto Challenges, 2013. [Online]. Available: https://cryptopals.com
[3] M. Bellare and P. Rogaway, *Introduction to Modern Cryptography*, UCSD CSE, 2005.
[4] I. Goldberg *et al.*, "End-to-end encrypted messaging," *Communications of the ACM*, vol. 58, no. 10, pp. 46–53, 2015.
[5] T. Frosch *et al.*, "SoK: Secure messaging," in *Proc. IEEE Symposium on Security and Privacy*, 2016.
[6] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*, Stanford University, 2020.
[7] R. Fielding, "Architectural styles and the design of network-based software architectures," Ph.D. dissertation, University of California, Irvine, 2000.
[8] A. Banks and E. Porcello, *Learning React: Modern Patterns for Developing React Apps*, O'Reilly Media, 2020.
[9] E. Brown, *Web Development with Node and Express*, O'Reilly Media, 2019.
[10] S. Tilkov and S. Vinoski, "Node.js: Using JavaScript to build high-performance network programs," *IEEE Internet Computing*, vol. 14, no. 6, pp. 80–83, 2010.
[11] F. J. Villanueva *et al.*, "WebSocket-based real-time communication systems," *IEEE Internet Computing*, vol. 23, no. 3, pp. 38–45, 2019.
[12] T. F. Lunt, "Access control policies for database systems," *IEEE Computer*, vol. 23, no. 6, pp. 38–46, 1990.
[13] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson Education, 2017.
[14] I. Goldberg, D. Stebila, and B. Ustaoglu, "Anonymity and one-way authentication in key exchange protocols," *ACM Transactions on Information and System Security*, vol. 13, no. 4, pp. 1–29, 2010.
[15] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," IETF RFC 5246, Aug. 2008.