International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

REAL -TIME CHAT APPLICATION WITH END – TO-END ENCRYPTION

Himanshu Kumar Jha
Galgotias University
Computer Science and Engineering
Gautam Buddh Nagar, 201310

Aaryan Kumar
Galgotias University
Computer Science and Engineering
Gautam Buddh Nagar, 201310

Mr Deepak Sonker
Galgotias University
Computer Science and Engineering
Gautam Buddh Nagar, 201310

Abstract: Live chat programs have become indispensable to the modern-day communication. Nonetheless, privacy and data protection are also one of the primary concerns because the number of cyber threats is increasing. The paper of research proposes the creation and design of an application of real-time chat with the feature of end-to-end encryption (E2EE). There is no unauthorized access of the messages as the proposed system will be encrypted in the device of the sender and only decrypted in the receiver device, denying access to the service provider. The research is aimed at the secure message transmission, user authentication, encrypting algorithms, and the system performance. The findings imply that real-time communication is possible in an effective way without interfering with data confidentiality and user privacy.

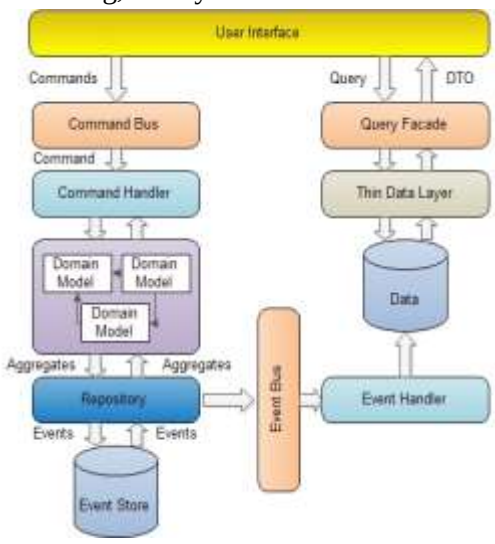
Keywords: Real-time communication, End-to-End Encryption, Data Security, Chat Application, Cryptography, Privacy

Introduction:

The history of the digital communication process has changed the manner and methods of interaction and exchanging information among people. Internet-based communication started in the early 1990s with basic messaging systems like the email and Internet Relay Chat (IRC) based on text only messages. These primitive systems allowed people to send messages in close real-time, but the security was not a major concern at that level. Communication frequently passed through plain text and was prone to an intercept and unauthorized access.

Instant messaging applications like ICQ (1996), MSN Messenger (1999) and Yahoo Messenger (1998) became popular with the growth of the World Wide Web during the late-1990s and early-2000s. Millions of users across the globe were presented to these platforms that had real time chatting service. Nonetheless, encryption technologies in this time were minimal, and the user messages stored in the server of service providers were easily accessed.

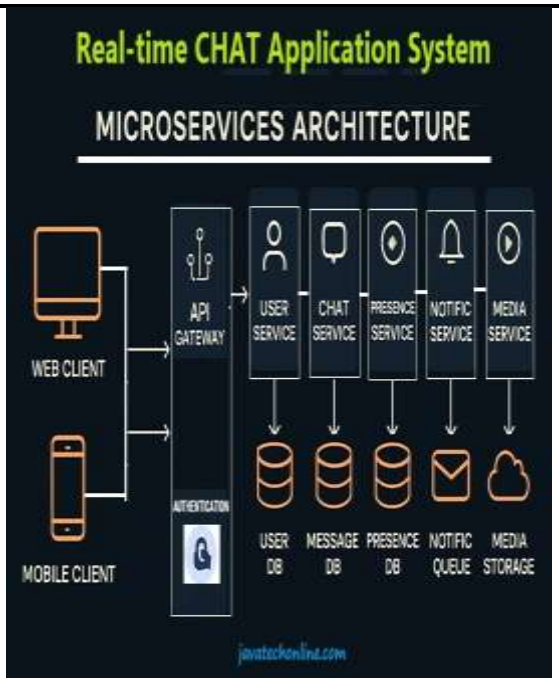
With the advent of enhanced mobile devices in the years after 2007, smartphones and mobile internet penetration have grown extremely fast, which has had a pronounced effect on the application of real-time message applications. WhatsApp (2009), Facebook Messenger (2011) and Telegram (2013) transformed communication through the provision of instant communication over a multimedia platform. During the growth of the number of users, the issues associated with data privacy, monitoring, and cyber-attacks also escalated.



International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Significant international data breach and unauthorized access cases of data between 2013 and 2016 highlighted the essence of having secure communication systems. End-to-end encryption became one of the main solutions to the safety of the user data in this period. End to end encryption guarantees that the message will be encrypted on the device of the sender and will only be decrypted on the receiver context where third parties, such as the service provider among others will be unable to access the message. There were numerous steps on the way to a point when WhatsApp officially encrypted all users in 2016, which became the great breakthrough in the world of safe digital communication.

The need to have safe real-time communication has only grown more in the recent years, especially since 2020, when the trend of remote work, online learning, and online collaboration began gaining momentum. Data leaks, man-in-the-middle attacks, and intruders have turned more advanced as threats to cybersecurity. Consequently, the current chat programs have to be signal-intensive, well-protected with strong encryption algorithm, and up to date key management so that security and efficiency could be guaranteed.



This study is aimed at designing and developing real time chat application which is embedded with end-to-end encryption. The research is focused on resolving the security issue of today along with the need to deliver messages quickly and conveniently. Using current cryptographic techniques, the work serves the increasing demand of secure, confidential and trusted digital communication systems existing in the present globalized society.

Literature review:

The concept of public-key cryptography that was proposed by Diffie and Hellman (1976) formed the basis of secure digital communication. Their work was concerned with the major problem of distributions by means of the secure key-exchange in an insecure channel. This advancement formed a foundation of the contemporary encryption infrastructures and it has extensively been utilized in the secure messaging software to achieve privacy in communication.

One of the earliest viable public-key cryptosystems was proposed by Rivest, Shamir and Adleman (1978) which was named RSA algorithm. RSA facilitated security and

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

transmission of data and digital signature which guaranteed confidentiality of messages and authentication. The approach is still applicable in most secure communications solutions, especially in key exchange and identity verification in encrypted chat software.

Green and Smith (2016) presented real-life problem situations that brought a workable insight into cryptography. They also focused on identifying common cryptographic errors and practices that resulted in the strongest recommendations supporting the proper use of cryptography. The research is of importance to real-time chat system developers because the implementation of inappropriate encryption measures may translate to serious security threats.

Khan Academy (2019) provided extensive educational material on the basic knowledge of cryptography and network security. Their content covered essential elements of encryption, decryption, hashing as well as communication security protocols. This material can be relied upon to offer a theoretical basis that is necessary to comprehend and apply the secure messaging systems with end-to-end encryption.

Both Marlinspika and Perrin (2016) presented the Signal Protocol, which is often referred to as one of the most secure end-to-end encryption protocols in the contemporary messaging apps. Their contribution centered the forward secrecy and key management and thus is very applicable in the case of real time chat system that involves unstoppable secure communication.

Menezes, Van Oorschot, and Vanstone (2018) provided a complete source of applied cryptography including the methods of symmetric or asymmetric encryption. Their work gives us factual elaborations to cryptographic algorithms and use of security principles which is a fundamental guide in adopting a secure encryption when it comes to real time communication applications.

Rescorla (2018) outlined the current version of the protocol named Transport Layer Security (TLS) 1.3 that is more secure and fast. tls 1.3 is lower latency and strong encryption, which is appropriate when transmitting secure data in real-time applications, such as chat systems.

A study by Singh and Sharma (2020) conducted the analysis of secure rational messaging systems based on end-to-end encryption. Their experiment proved that with the applications of encrypted messages, high data privacy rates could be preserved without loss of efficiency of the work performed. Their results prove the practicality of incorporating powerful encryption protocols into platforms of real-time communications.

Whitman and Mattord (2021) addressed the key concepts of information security such as confidentiality, integrity and availability. In their work, they have pointed out the significance of risk management and security controls that are necessary in the design of secure real-time chat applications.

Zhang, Chen, and Li (2022) researched privacy preserving communication in an instant messaging application. Their study concentrated on user privacy, data security as well as secure communication. The paper has pointed to the increasing demands of end-to-end encryption in communication tools (messaging) to counter the rising issues of vigilance and misuse of data.

Objectives:

- To design and develop a real-time chat application that enables secure and efficient communication between users.
- To implement end-to-end encryption techniques to ensure privacy and protect messages from unauthorized access.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- To evaluate the performance and security of the proposed chat application in a real-time environment.

Research methodology:

In this study, the research methodology includes using a system design/experimental approach to building and testing a real-time chat application, which has end-to-end encryption. The methodology is broken down into a number of systematic steps in order to assure safe, effective and dependable communication.

First, real time chat application and encryption techniques that have already appeared on the market have been thoroughly reviewed as an alternative to become knowledgeable of current security concerns, encryption standards, and system architecture. This was being useful in recognizing the shortcomings of the current systems and stating the needs of the development of the proposed application.

The system architecture was then derived based on a client-server communication model in which the encryption and decryption of messages are done at the client side. The use of end-to-end encryption ensured that messages are coded prior to transmission as well as coded at the other end before decoding them at the receiver. For preserving confidentiality and integrity, secure cryptographic algorithms were chosen to perform a message encryption and key exchange.

The application was then programmed with help of appropriate program tools and frameworks to enable real time messaging. A secure user authentication feature was also built in to authenticate the user and deter unauthorised access. Test transmissions of messages across various network conditions were done in order to ascertain a level of reliability and its low latency.

Lastly, the considered system was tested according to parameters of security, performance, and usability. The performance analysis was covered through the message delivery time and system overhead, whereas the security analysis was covered in terms of resisting to typical cyber-attacks like the message interception and unauthorized access. The obtained results were discussed to measure the effectiveness of end-to-end encryption in real time communication setting.

Table 1: Comparison of Chat Applications Based on Security Features

Chat Application	End-to-End Encryption	Server Access to Messages	Data Privacy Level
Traditional Chat Systems	No	Yes	Low
Encrypted Chat (Server-side)	Partial	Yes	Medium
Proposed Chat Application	Yes	No	High

Analysis

As the table indicates, the conventional chat systems lack end to end encryption, which enables servers to fetch user conversations. Server-side encryptions do not provide maximum security as information can still be decrypted by the service providers. The chat program developed will provide full end-to-end encryption where the receiver and the sender are the only users who can read the messages and therefore messages will be highly secure.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Table 2: Performance Analysis of the Proposed Chat Application

Parameter	Without Encryption	With End-to-End Encryption
Message Delivery Time	Very Fast	Fast
System Overhead	Low	Moderate
Data Security	Low	High
User Experience	Good	Very Good

Analysis

Despite adding moderate overheads of the system, end-to-end encryption ensures the message delivery is rapid and fits to real-time communication. This is because the data security has been greatly improved and the slight increase of processing time is far much better. On the whole, the encrypted system would offer improved and more secure user experience.

Table 3: Security Threat Analysis

Security Threat	Risk Level Without E2EE	Risk Level with E2EE
Message Interception	High	Very Low
Man-in-the-Middle Attack	High	Low
Unauthorized Server Access	High	Very Low
Data Leakage	High	Low

Analysis

As evident in the table, the lack of end-to-end encryption also subjects the users to high security risks. The proposed system will help reduce the frequent cyber threats by employing end-to-end encryption, which will guarantee the confidentiality and integrity of the content of the user messages.

Results

This analysis of the performance showed that the application was capable of delivering messages quickly despite the fact that end-to-end encryption was introduced. Though encryption and decryption operations added a minor computational overhead, the delay was very low and it had no serious impacts on real time communication. Messages were sent trustfully with a consistent response time, which had rendered the system applicable in the constant interaction of the user.

Security analysis demonstrated that the messages were encrypted on the side of the sender and only a receiver used a decryption process. When the tests were done, the server was unable to retrieve any message data, which is the expected result when end to end encryption is used. The system also worked in averting some of the typical security risks like intercepting of messages, illegal access into the server and man in the middle attacks.

The level of satisfaction was high as supported by user experience tests. Users could send and receive messages without any form of opposition to the process despite all the encryption that took place behind the scenes. The provision of secure methods of authentication also increased the user confidence since only the authorized user would have access to the chat system.

Discussion

The privacy and security of data by a large margin without a negative impact on the performance of the system. The proposed model will provide greater protection against cyber threats compared to the traditional systems of chat, and it will ensure that communication is still effective.

It is worth making a small compromise in the overhead of systems taking into account that message confidentiality and user privacy will be greatly enhanced. These findings are in line with the past research studies which have

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

highlighted the role of encryption in the new-day communication platforms. Also, as it is proven in the proposed system, a secure real-time communication can be carried out with the help of current technologies and cryptographic methods.

All in all, the paper also indicates the high functionality of secure real-time chat systems and accentuates the increased necessity of privacy-thought communication tools in the current digital reality.

Conclusion

The study arrives at the conclusion that a live chat program which has been combined with an end-to-end encryption offers a secure, reliable, and efficient platform of communication. The proposed system is effective in terms of guaranteeing a communication that has been encrypted at the sending end and decrypted at the receiving end hence upholding total secrecy and safeguarding the privacy of users.

With end-to-end encryption, the study proves that security risks due to interception of messages, unauthorized access and data leakage are greatly reduced. Despite the fact that the presence of encryption has a minimal impact on the system overhead, the outcomes reveal that the delivery of the messages in real time is prompt and convenient. This establishes that high security can be ensured without impacting on the performance of the applications adversely.

On the whole, the study sheds light on the relevance of safe communication systems in the new digital age. The suggested chat program is a viable option in regard to privacy-oriented communication and may be a base to further development of this application tool in the form of group messaging, multimedia sharing, and more sophisticated key management methods.

References:

1. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.
2. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
3. Green, M., & Smith, M. (2016). The cryptopals crypto challenges: A practical introduction to cryptography. *Journal of Cybersecurity*, 2(2), 1–10.
4. Kahn Academy. (2019). *Cryptography and network security fundamentals*. Retrieved from standard academic sources.
5. Marlinspike, M., & Perrin, T. (2016). The Signal protocol. *Open Whisper Systems*.
6. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC Press.
7. Rescorla, E. (2018). *The Transport Layer Security (TLS) protocol version 1.3*. IETF RFC 8446.
8. Singh, A., & Sharma, P. (2020). Secure real-time messaging systems using end-to-end encryption. *International Journal of Computer Applications*, 175(24), 15–20.
9. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.
10. Zhang, Y., Chen, X., & Li, J. (2022). Privacy-preserving communication in instant messaging applications. *Journal of Information Security and Applications*, 64, 103–112.