IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, May 2026
Impact Factor: 8.2

Enhancing End-to-End Encrypted Messaging : A Hybrid Classical-Post Quantum Approach with Real-Time Multi- User Support

D. Shashikala[1] and C. Jyothsna[2]
[1]PG scholar, Department of Computer Science & Engineering
[2]Associate Professor, Department of Computer Science & Engineering
Chadalawada Ramanamma Engineering College (Autonomous), Tirupati.

Abstract: *Enhancing End-to-End Encrypted Messaging : A Hybrid Classical-Post- Quantum Approach with Real-Time Multi- User Support is a way for people to send messages to each other. It is called a communication platform. It helps users send encrypted messages in time. This platform uses new ways of hiding messages to keep them secret. It wants to make sure that only the people who are supposed to see the messages can see them. The people who made this platform used Python to build it. They used Flask and Socket.IO to make it work on the web. They also used ways to hide messages like DES and RSA. They even used some ways like Kyber and Dilithium. These new ways are being checked by NIST to make sure they are good. Users can. Join groups to talk to each other. They can choose how they want to hide their messages. The system is also flexible so new ways of hiding messages can be added later. This project shows that I can use new ways of hiding messages together. It wants to help us send messages safely when computers get much better at figuring out secrets. The platform is designed to keep messages secret and safe. It uses algorithms like El Gamal and Falcon. These algorithms help keep messages secret. The platform also supports users at the same time. It is a way for people to send messages to each other without worrying about others seeing them. This project is important because it helps us prepare for the future. It shows us how to use new ways of hiding messages together. This will help us send messages safely when computers get much better. The End-to-End Encrypted Messaging platform is an example of how I can use technology to keep our messages secret and safe.*

Keywords: Secure Chat Application , Post-Quantum Cryptography ,Hybrid Cryptography , NIST PQC Algorithms , Socket.IO

I. INTRODUCTION

Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post- Quantum Approach with Real-Time Multi-User Support is a deal for people who want to keep their online conversations private. This thing is a step forward in secure communication technology. It introduces a way of encrypting messages that uses many different algorithms. People are really worried about their privacy these days because of all the hacking and spying that is going on. Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post- Quantum Approach with Real-Time Multi-User Support is a solution to these problems. It is a kind of chat application that uses eighteen different encryption algorithms to keep messages safe. These algorithms are a mix of new methods.

The Enhancing End-to-End Encrypted Messaging system is a deal because it helps keep our messages safe. I know that using one way to encrypt messages is not enough because it can be easily broken. Most messaging platforms use one or two encryption methods. The Enhancing End-to-End Encrypted Messaging system uses many different ways to encrypt messages. It uses methods like DES, ElGamal and RSA. It also uses methods like CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, SABER, NewHope, FrodoKEM, NTRUEncrypt, NTRUPrime, Classic McEliece, BIKE, HQC,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, May 2026 Impact Factor: 8.2

Rainbow, SPHINCS+, CSIDH and Picnic. This means that even if someone breaks one of the encryption methods the message is still safe. The Enhancing End-to-End Encrypted Messaging system is useful for things.
It is useful for businesses that need to keep their conversations secret.
It is useful for schools where students can learn about encryption.
It is useful for security researchers who want to test encryption methods.
It is also useful for people who want to keep their messages private.
The Enhancing End-to-End Encrypted Messaging system is ready for the future because it uses - quantum algorithms.

II. EXISTING SYSTEM

The existing end-to-end encrypted chatting applications are designed to securely transmit sensitive information while preventing unauthorized access and malicious intrusions. These applications play a vital role in organizational environments, where employees frequently exchange confidential messages that may include trade secrets and critical business information. Current systems employ the OR Diffie–Hellman Key Exchange (ORDEX) algorithm to establish secure communication channels between users. To enhance security, multiple key exchange processes and additional cryptographic layers are incorporated. Although this approach strengthens protection, it introduces increased computational complexity, which negatively impacts application performance and responsiveness.
To further reinforce security, the existing architecture integrates the ORDEX algorithm with the Extended Triple Diffie–Hellman (X3DH) protocol and the Double Ratchet mechanism. This combination ensures secure session establishment, forward secrecy, and protection against key compromise. Message confidentiality is maintained using the Advanced Encryption Standard (AES) for encrypting the actual message content. While this layered cryptographic framework provides strong security guarantees, it has been observed that such implementations are significantly slower—up to a thousand times—when compared to secure chatting applications based on Elliptic Curve Diffie–Hellman (ECDH) key exchange. This performance limitation presents challenges in scenarios that require both high levels of security and real-time communication efficiency, highlighting the need for optimization in existing secure chat systems.

III. PROPOSED SYSTEM

The Enhancing End-to-End Encrypted Messaging system is a way to make sure that messages are safe and secure. This system Enhancing End-to-End Encrypted Messaging: A Classical-Post- Quantum Approach with Real-Time Multi-User Support solves all the problems that other secure chat applications have. It does this by using a lot of encryption methods. Enhancing End-to-End Encrypted Messaging: A Classical-Post- Quantum Approach with Real-Time Multi-User Support uses eighteen different encryption algorithms. This gives users a lot of options to keep their messages safe. Other systems only use one encryption method.. Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post- Quantum Approach with Real-Time Multi- User Support lets users switch between different encryption methods for each message. This makes it very hard for someone to figure out the code.
Support is the Random Mode. This mode uses a random number generator to choose a different encryption method for each message. This means that it is almost impossible to figure out the pattern of the encryption methods. The system uses a number generator to make sure that the encryption methods are always changing. The Enhancing End-to-End Encrypted Messaging system is made up of different parts that work together. The backend server handles all the messages and stores the data. The frontend is what the users see and interact with. There is also a desktop client that gives users another way to use the system. All of these parts work together to make sure that messages are safe and secure. The Enhancing End-, to-End Encrypted Messaging system is special because it can switch between encryption methods. This makes it one of the ways to send messages.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, May 2026
Impact Factor: 8.2

IV. ANALYSIS

This chapter is about the Enhancing End-to-End Encrypted Messaging: A Classical-Post- Quantum Approach with Real-Time Multi- User Support system. It looks at what the system needs to work what users want from it and what hardware and software are required. The Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post-Quantum Approach with Real-Time Multi- User Support system also needs a flowchart to show how it operates. This part of the project is very important because it sets the foundation for the system. By looking at what the system needs to do and how it will work I can understand what the Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post- Quantum Approach with Real-Time Multi- User Support system must accomplish how it will operate and what resources are necessary for it to be implemented and deployed.

The Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post- Quantum Approach with Real-Time Multi-User Support system is a secure messaging platform. It uses encryption algorithms and allows many users to communicate in real-time. To understand what the system needs I have to look at things. These include what the system should do how it should work, how users will interact with it and what technical resources are needed to support it. By doing this I can make sure that the Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post- Quantum Approach with Real-Time Multi- User Support system meets all the requirements and is what the users expect. There are key steps in this part of the project. First I gather information from users, experts and existing systems. Then I analyze this information to identify what the system really needs fix any conflicts and decide what features are most important. Next I document these needs in a way so that they can be used to design and implement the Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post- Quantum Approach with Real-Time Multi- User Support system. Finally I review these needs to make sure they are complete, consistent and can be achieved within the projects limits. The Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post- Quantum Approach with Real-Time Multi- User Support project is complex because it involves cryptographic algorithms real-time communication and support for many users. The system has to handle encryption standards while still working well provide a user-friendly interface while offering advanced security features and support many users at the same time while keeping messages secure and private. This chapter looks at all these things in detail to give a picture of what the Enhancing End-to-End Encrypted Messaging: A Hybrid Classical-Post- Quantum Approach, with Real-Time Multi- User Support system needs and how it will work.

4.1 Software Requirements Specification

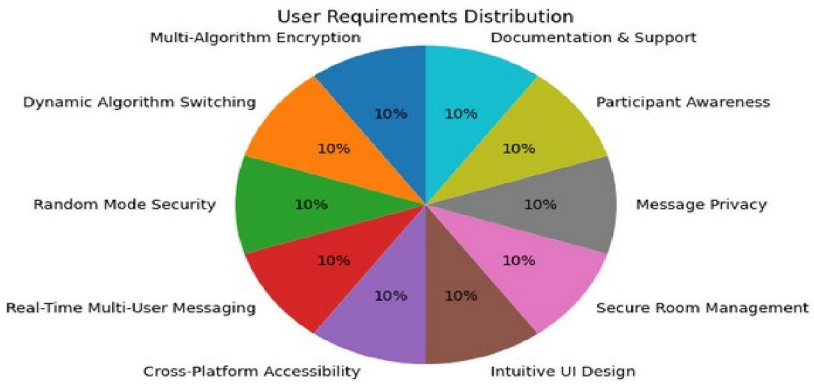

Fig:1 Software Requirements Specification

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, May 2026
Impact Factor: 8.2

Users should have access to documentation that explains how to use the system from basic instructions for new users to advanced features for experienced users. System notifications and error messages should be clear, helpful and provide actions to take so users can solve problems quickly. Use the systems features effectively. Enhancing End-to-End Encrypted Messaging is, about making sure that users have a secure and easy-to-use communication platform. The system must keep user communications private. All messages should be encrypted when they are sent and if necessary, when they are stored. Information about the encryption, like which algorithm is used should not be visible in a way that could help others figure out the encryption patterns.

Hardware Requirements

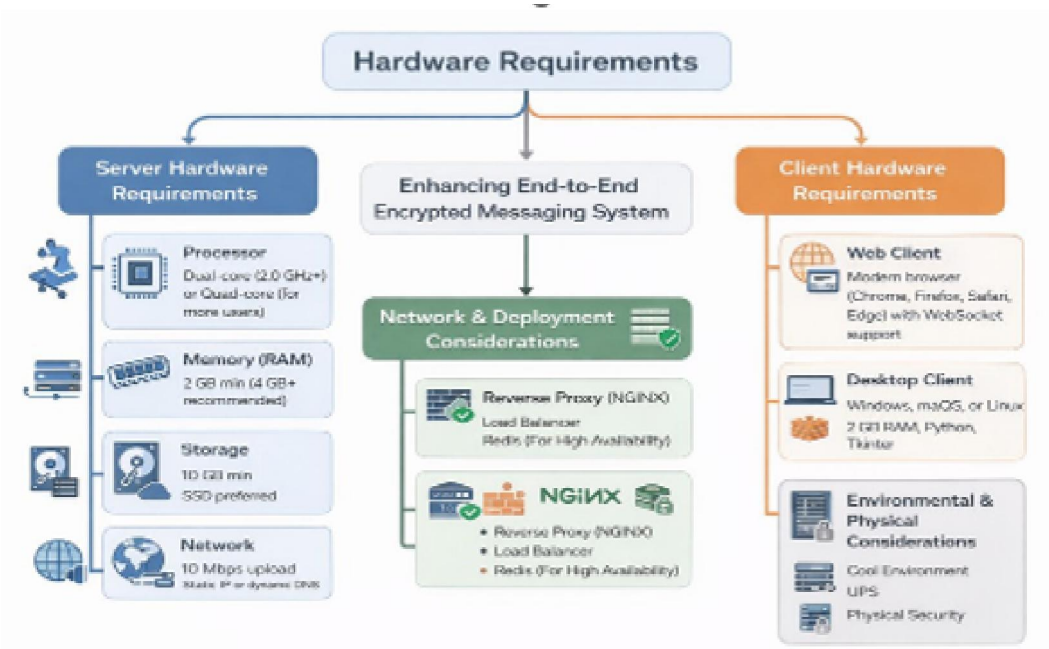

Fig 2: Hard ware Requirements

The hardware that the Enhancing End-to-End Encrypted Messaging system needs is very important for it to work properly. The Enhancing End-to-End Encrypted Messaging system has requirements for the server and the client. These requirements are divided into two categories: the minimum that the Enhancing End-to-End Encrypted Messaging system needs to work and what is recommended for the Enhancing End-to-End Encrypted Messaging system to work well.

V. CONCLUSION

The messaging platform can be made better in the future. This will make it easier for users to use the platform. The platform will still be very secure. One thing that can be done is to make apps for different devices. These apps can be made using React Native or Flutter. This way the apps will work on iOS and Android devices. I can also make desktop apps using Electron. These apps will work on Windows, macOS and Linux. The website version of the platform can also be improved. This will make it easier for people to use the platform on their browsers. They will even be able to use it when they are not connected to the internet. The secure messaging platform is going to be developed in a steps. I have a plan with three parts. This plan makes sure the platform gets better and better without any problems. I want to make sure the platform is stable secure and can handle a lot of users.

DOI: 10.48175/IJARSCT-35389

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, May 2026
Impact Factor: 8.2

REFERENCES

[1]. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. 35th Annual Symposium on Foundations of Computer Science (FOCS), Santa Fe, NM, USA, Nov. 1994, pp. 124–134.

[2]. T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature verification and message encryption," in Advances in Cryptology—EUROCRYPT '88, Berlin, Germany: Springer, 1988, pp. 419–453.

[3]. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[4]. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[5]. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Advances in Cryptology—CRYPTO '84, Santa Barbara, CA, USA: Springer, 1985, pp. 10–18.

[6]. National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197,Nov.2001.[Online].Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[7]. P. Bos et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in Proc. IEEE European Symposium on Security and Privacy (EuroS&P), London, U.K., Sep. 2018, pp. 353–367.

[8]. L. Ducas et al., "CRYSTALS-Dilithium: A lattice-based digital signature scheme," Transactions on Cryptographic Hardware and Embedded Systems, vol. 2018, no. 1, pp. 238–268, Jan. 2018.

[9]. P.-A. Fouque et al., "Falcon: Fast-Fourier lattice-based compact signatures over NTRU," Transactions on Cryptographic Hardware and Embedded Systems, vol. 2018, no. 4, pp. 235–260, Oct. 2018.

[10]. J. Bos et al., "SABER: Mod-LWR based key encapsulation mechanism," Sep. 2023. [Online].

[11]. Available: https://saber.org/

[12]. D. J. Bernstein et al., "NewHope: Post-quantum key exchange," May 2023. [Online]. Available: https://newhopecrypto.org/

[13]. J. Bos et al., "Frodo: Take off the ring! Practical quantum-secure key exchange from LWE," in Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS), Vienna, Austria, Oct. 2016, pp. 1006–1018.

[14]. J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in Algorithmic Number Theory Symposium (ANTS), Portland, OR, USA: Springer, Jun. 1998, pp. 267–288.

[15]. N. Aragon et al., "NTRU Prime: Reducing attack surface at low cost," in Selected Areas in Cryptography (SAC 2015), LNCS, vol. 9564, Springer, 2015, pp. 235–260.

[16]. National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization," 2016. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[17]. T. Avşar and M. Kara, "Real-time secure group messaging," in Proc. International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, Feb. 2023, pp. 142–147.