IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

QUANTUM ENCRYPTED MESSAGING SYSTEM: A SECURE COMMUNICATION PLATFORM USING POST QUANTUM CRYPTOGRAPHY

[1] Lakshmikanth R, [2] Sandhya J, [3] Srinivasulu R, [4] Mrs ThamaraiSelvi

[1-3] Final year Student, Department of AIML, [4] Assistant Professor, Department of AIML, [1]Bangalore Technological Institute, Bangalore, India.

Abstract : The rise of quantum computing brings serious risks to current encryption systems, making it essential to create communication systems that can withstand attacks from quantum computers. This paper introduces the design of a secure messaging app that combines Quantum Key Distribution (QKD) with post-quantum cryptographic methods to guarantee complete privacy and reliability in digital messages. In addition to its strong security features, the system also uses artificial intelligence tools like real-time translation between languages and smart conversation helpers that understand context, making the app more user-friendly and accessible. The app is built to work on different devices and operating systems, allowing it to be easily used in various environments. The system will be tested through repeated development cycles, stress tests, and user feedback to improve both its performance and ease of use. The platform brings together quantum-secure communication and AI-driven user interaction, offering a flexible and scalable solution for secure digital messaging in the future.

Keywords: Quantum Key Distribution (QKD), Post-Quantum Cryptography, Secure Messaging, Artificial Intelligence, Real-Time Translation, Human-Computer Interaction.

I INTRODUCTION

The growing use of digital communication has raised more worries about security, especially with the rise of quantum computing, which could make traditional encryption methods ineffective. Algorithms like RSA and ECC, which are used to protect secure messaging today, are becoming more vulnerable to attacks from quantum computers. This creates a pressing need for new security solutions that can withstand quantum threats.

This paper presents a new messaging app that uses Quantum Key Distribution (QKD) and post-quantum cryptography to offer strong, unbreakable privacy.

In addition to focusing on security, the app makes communication easier with AI features like real-time translation between languages and smart assistants that understand context. This combination of strong quantum security and smart user tools makes the app more resistant to hacking, user-friendly, and ready for the future of digital communication.

II LITERATURE SURVEY

Quantum key distribution (QKD) is a crucial part of quantum cryptography that helps fix the weaknesses of traditional encryption when facing attacks from quantum computers. The BB84 protocol and other early discoveries showed how quantum mechanics can be used to securely share keys and detect if someone is eavesdropping.[1] Investigating Quantum Key Distribution, BB84 has become a key part of real-world QKD systems used in fiber networks, satellites, and mixed setups.[2] This has been supported by further research that has confirmed its role in securing communications as we move into the post-quantum era. Alongside QKD, there's also work on post-quantum cryptography (PQC), which provides security at the software level without needing special hardware. Studies show that lattice-based and code-based methods are practical options that can be used on existing systems and work well with QKD.[4] To solve the problems of each method alone, hybrid approaches that mix QKD with PQC have been proposed. These strategies aim to balance performance, cost, and scalability. The use of these methods in secure messaging has also been explored. One study proposed a quantum-encrypted messaging system that considers user experience and key management, combining NTRU-based encryption with AES to offer quantum resistance.[3] Systematic reviews of quantum cryptography also highlight the

importance of combining QKD with modern cryptographic protocols to ensure security in future networks. Although most messaging apps like Signal, WhatsApp, and ProtonMail use end-to-end encryption, they are still vulnerable to quantum attacks. The literature shows that there's a lack of systems that include user-friendly features like conversation support and AI-based translation along with quantum-secure encryption.[5] The proposed application fills this gap by integrating QKD, PQC, and AI-driven usability improvements into a scalable, cross-platform secure messaging framework, offering a new and valuable solution.

III OBJECTIVES

1.Establish Quantum-Resistant Security: Use Quantum Key Distribution (QKD) to allow users to share keys that cannot be broken. Protect messages from both traditional and future quantum attacks by using post-quantum cryptography. Make sure all data is secure and encrypted from end to end, helping to keep the messaging platform safe against possible quantum threats.

2. Improve User Privacy: Keep user data and conversations private so only the right people can access them, even those with advanced computing skills. Prevent attacks where someone secretly listens in or intercepts messages, even if the attacker has access to quantum technology.

3. Include Cutting-Edge AI-Powered Features: Add real-time translation so users can easily talk to each other in different languages. Use smart chat assistants to make interactions more engaging, automate tasks, and provide helpful responses.

4. Provide a Smooth and Easy-to-Use Experience: Make sure all the new AI and security features work in the background without needing users to have technical knowledge. Keep the system fast, reliable, and simple to use, even as it handles complex quantum and AI technologies.

5. Digital Communications That Are Future-Proof: Create a messaging system that can handle new security challenges as quantum computing develops. Set a new standard for secure, smart, and user-cantered digital communication in a world that is becoming more connected.

IV MOTIVATION

1. Threats from Quantum Computing: The encryption methods currently used in most messaging apps could be broken by the fast growing power of quantum computers. There is a pressing need to ensure that digital communications stay secure even as quantum computing advances.

2. Growing Privacy and Security Concerns People are increasingly aware of the risks to their privacy and want stronger protection for their personal and work-related messages. Recent high profile data breaches and indices of surveillance have exposed weaknesses in current security practices.

3. Current Messaging Apps' Limitations Most popular messaging apps rely on traditional encryption methods, which may not be safe once quantum computers become common. Few apps offer strong security features that can resist attacks from quantum technology.

4. The Need for User-Friendly and Smooth Solutions. Security improvements should not Ake the app harder to use or require users to ave technical skills. There is a growing demand for messaging services that are both safe and easy to use.

5. The Need for Intelligent Features like real time translation and smart chat assistants are now expected by users, who want more than just secure messaging. Adding AI based tools can greatly improve how accessible and engaging messaging apps.

6. Safeguarding Private Communications For individuals, businesses, governments, and organizations that deal with private or sensitive information, secure messaging is crucial. Inan increasingly digital world, it's vital to keep communications private and trustworthy.

7. Keeping Up with Technological Development By actively using AI and quantum technologies, the app can stay ahead of trends and potential security risks.as quantum computing becomes more widespread, taking early steps to adopt quantum safe solutions can give a competitive edge.

V METHODOLOGY

The system is built with two main goals: better usability and strong security that can handle future quantum threats. It's structured into four key parts: evaluation, a cross-platform framework, smart services, and a secure core.

At the heart of the system is a strong security layer that combines post-quantum cryptography (PQC) with ideas from quantum key distribution (QKD).

This ensures security during the setup of keys and verification of identities. Lattice-based methods, like CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for authentication, provide quantum resistance.[6] After keys are shared, AES-256 is used to encrypt messages. To reduce risks from long-term exposure, session keys are often changed, which is similar to the forward secrecy feature in QKD.

The system also uses AI tools to make it more accessible and user-friendly.AI-powered natural language processing (NLP) enables real-time translation between different languages, helping people from all around the world communicate easily. Smart chat assistants, which understand context, offer helpful and flexible support during conversations.The system works smoothly on different platforms like desktops, mobile devices, and the web.It uses a modular design that makes it easy to scale, integrate

with other systems, and adapt to new user needs.The development process is ongoing and user-focused.

Working prototypes are tested for security, speed, and performance. User input helps improve both the security features and the usability of the system. This approach ensures a balance between strong technical security and easy-to-use interactions.By combining QKD ideas, PQC methods, AI improvements, and cross-platform design, this approach creates a communication platform that is both ready for the future and meets the modern user's expectations for ease of use and security.

VI DESIGN

The data flow diagram of the proposed system shows how different parts of the system work together (Figure 1).[3] It includes user devices, application services, a security layer, and the backend system. Messages from iOS and Android apps go through secure connections to a central messaging service, which acts as the main communication center. This service connects with AI features like real-time translation, smart chat helpers, predictive text, and auto-reply suggestions to improve the user experience. At the same time, the messaging service talks to the security layer, where quantum key distribution creates encryption keys. These keys are then handled by post-quantum cryptographic algorithms to protect data against future threats from quantum computing. Once messages are processed and encrypted, they go through the server backend and are stored safely in a database. This flow explains how quantum-secure encryption and AI tools are used together to build a smooth, cross-platform messaging system.

VII EVALUATION

The suggested messaging app uses a mixed approach that balances strong security with ease of use by combining artificial intelligence services with quantum-safe encryption.

From a security perspective, it is strong against both traditional and future quantum attacks by using lattice-based post-quantum cryptography along with key renewal methods inspired by quantum key distribution. The app regularly changes session keys, which lowers the risk of long-term key exposure and fixes issues found in earlier studies, unlike older systems that rely on RSA or ECC encryption.

The app also focuses on making the service easy to use, which is often ignored in cryptography research.It includes AI tools like real-time translation, predictive text, and smart assistants to help users communicate more easily and make secure messaging feel like the convenient experience people expect from popular apps. Because of this mix of security and user-friendly features, the app works well for people around the world and offers both technical protection and practical use.The system also solves scalability problems that have been talked about in previous studies.

Its software-based design uses post-quantum algorithms that can work on existing networks, making it accessible on desktops, the cloud, and mobile devices. Unlike hardware-based quantum key distribution systems, which are limited by infrastructure and cost, this approach is more flexible. The app's modular design handles complex tasks without making the user experience worse, and ongoing testing and improvements will help find the best balance between strong security and quick response times.This platform connects human-centred design with quantum-safe communication, making progress over earlier work.

The combination ensures that future messaging apps can include both security and ease of use as must-have features, rather than having to choose between them. The conversation highlights how important hybrid models are in creating communication systems that are both technologically reliable and focused on the user, ready for the quantum future.

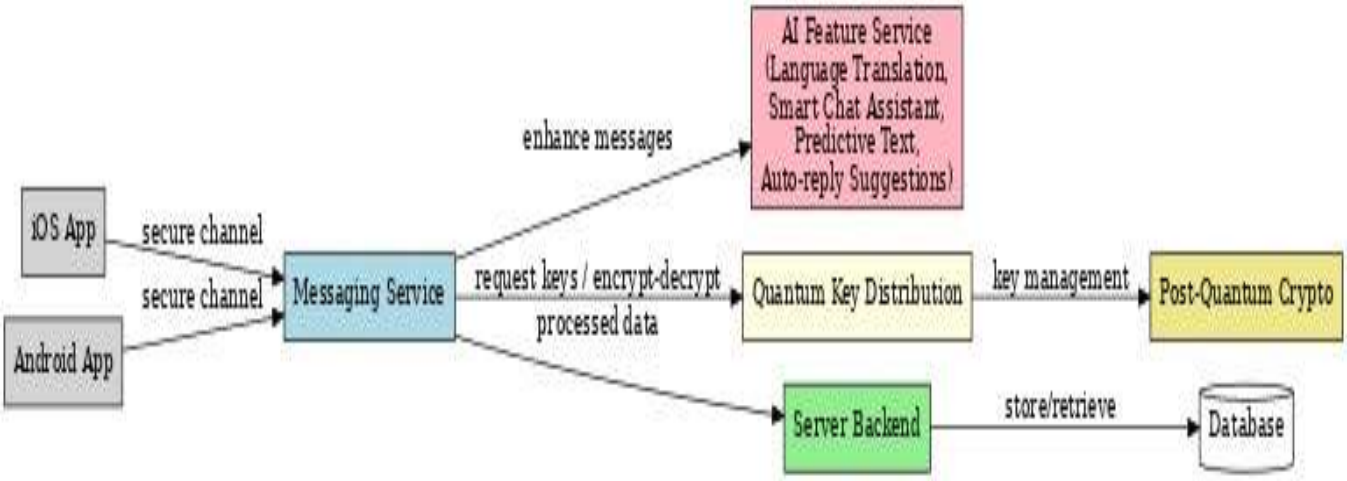

Figure 1: Data flow diagram

VIII RESULT

The proposed system is deliver a messaging platform that is secure, capable of growing with demand, and easy for users to navigate. It is designed to handle both existing and potential risks in digital communication. The app aims to perform well in real-world situations while protecting against threats from adversaries who may use quantum computing. This is achieved through the use of post-quantum cryptography and techniques that draw inspiration from quantum key distribution.

It is believed that the inclusion of AI-powered features will encourage more users around the world to adopt the platform.These features will make the experience more user-friendly by offering smart conversation assistance and seamless support for multiple languages.

IX CONCLUSION

In summary, this paper brings together artificial intelligence and quantum-safe cryptography in a new way to ensure secure digital communication.

The suggested application creates a balanced approach where both AI and security are optimized, unlike many current systems that focus on either user experience or strong encryption. This sets a benchmark for future research and development in safe, smart messaging tools, and positions the platform as a communication solution that is ready for the quantum era.

REFERENCES

[1] S. S. Gujar, "Exploring Quantum Key Distribution," 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI), Wardha, India, 2024.

[2] J. Gulati and R. Raman, "Quantum Key Distribution: Harnessing the Power of BB84 for Secure Communications in the Post-Quantum Era," 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies, Pune, India, 2024.

[3] R. G. Sharon, A. S. Kumar, A. Mayan and A. Catherine, "Quantum Encrypted Messaging Application: Harnessing Quantum Mechanics for Secure Communication," 2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), Dehradun, India, 2024.

[4] K. -S. Shim, B. Kim and W. Lee, "Research on Quantum Key, Distribution Key and Post-Quantum Cryptography Key Applied Protocols for Data Science and Web Security," in Journal of Web Engineering, vol. 23, no. 6, pp. 813-830, September 2024.

[5] Durr-E-Shahwar, M. Imran, A. B. Altamimi, W. Khan, S. Hussain and M. Alsaffar, "Quantum Cryptography for Future Networks Security: A Systematic Review," in IEEE Access, vol. 12, 2024.

[6] O. Alibrahim, "Unveiling Samsung Quantum Galaxy: Securing Smartphones With Quantum and Post-Quantum Cryptography," in IEEE Access, vol. 13, pp. 73202-73218, 2025.