International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Secure Chat Application using Quantum Cryptography Simulation

1. Swapnil Pagar
Department of Computer Engineering
SND College of Engineering and Research Centre
Yeola, Nashik, Maharashtra, India

2. Gore Sahil
Department of Computer Engineering
SND College of Engineering and Research Centre
Yeola, Nashik, Maharashtra, India

3. Arote Rohit
Department of Computer Engineering
SND College of Engineering and Research Centre
Yeola, Nashik, Maharashtra, India

4. Shinde Mayur
Department of Computer Engineering
SND College of Engineering and Research Centre
Yeola, Nashik, Maharashtra, India

5. Kanade Poonam
Department of Computer Engineering
SND College of Engineering and Research Centre
Yeola, Nashik, Maharashtra, India

Abstract **- This study introduces a secure chat application based on quantum cryptography simulation to strengthen the privacy and security of online messaging. The proposed system combines traditional chat functionality with Quantum Key Distribution (QKD) to safeguard conversations against eavesdropping and impersonation attacks. Using the BB84 quantum protocol, the application performs secure key exchange in a simulated environment, ensuring that only authorized users can access the messages. Simulation results demonstrate that the system achieves significantly better security than conventional encryption methods. This research provides a practical and straightforward framework for quantum-enhanced secure communication, highlighting its feasibility for real-world deployment in the future.**

Keywords - Quantum Cryptography, Quantum Key Distribution, QKD, BB84 Protocol, Secure Chat Application, Quantum Simulation, Secure Messaging, Eavesdropping Protection, Data Privacy, Encryption, Quantum Security, Secure Communication

I. INTRODUCTION

This The rapid growth of digital communication has made messaging apps and online platforms an essential part of daily life. However, this increase has also raised serious security concerns, such as data interception and unauthorized access. Traditional encryption methods, which rely on complex mathematics, are becoming vulnerable to powerful computers and future quantum computers.

Quantum computing can break many current encryption techniques, like RSA, using algorithms such as Shor's algorithm. To address this challenge, researchers are turning to quantum cryptography. Quantum Key Distribution (QKD) provides a highly secure way to share encryption keys by using the laws of physics. Any attempt to eavesdrop can be easily detected.

This project develops a Secure Chat Application that simulates quantum cryptography using the BB84 protocol. Since real quantum hardware is not easily available, the system simulates the complete process of quantum key exchange in a normal computing environment. The generated keys are then used with AES encryption to ensure secure real-time messaging between users.

The application is designed with a simple and user-friendly interface, supporting multiple platforms. It demonstrates how quantum cryptography principles can be practically applied to create safer digital communication systems.

II. PROBLEM DEFINITION

In today's fast-paced digital era, the exponential growth of online communication platforms has significantly intensified the challenges associated with secure data exchange. As individuals and organizations increasingly rely on instant messaging for personal and professional interactions, the threat landscape has expanded dramatically. Cyber threats such as eavesdropping, data tampering, message interception, and unauthorized access have become more sophisticated, putting users' privacy and sensitive information at constant risk. Traditional cryptographic methods, which form the foundation of most existing chat applications, depend heavily on mathematical complexity for security. Although these approaches have served reliably for decades, they are now facing serious limitations due to rapid advancements in computing power. Particularly concerning is the emergence of quantum computers, which are expected to break widely used public-key algorithms like RSA and Diffie-Hellman, rendering current encryption techniques potentially obsolete.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Moreover, the majority of modern chat platforms rely on classical encryption techniques for key exchange that lack any built-in mechanism to detect active interception or eavesdropping attempts. This critical shortfall leaves users unaware of whether their conversations are being secretly monitored, creating a substantial security gap in real-world communication.

To overcome these pressing challenges, the main objective of this project is to design and develop a robust secure chat application that incorporates quantum cryptography principles by simulating the BB84 protocol for secure key distribution. The proposed system seeks to address the shortcomings of conventional cryptography by delivering superior levels of confidentiality, integrity, authenticity, and forward secrecy. It will facilitate seamless, real-time communication across multiple platforms, offering strong defense against prevalent cyber threats without requiring users to depend on any additional security tools or plugins.

III. LITERATURE SURVEY

[1] Rubio García, C., Cano Aguilera, A., Stan, C., Vegas Olmos, J. J., Rommel, S., & Monroy, I. T. (2025). Enhanced Network Security Protocols for the Quantum Era: Combining Classical and Post-Quantum Cryptography, and Quantum Key Distribution. IEEE Journal on Selected Areas in Communications, 43(8), 2765–2781.

[2] Li, Li, Zhang, Wen, Du, Chen, and Ma (2018) present a foundational survey on Quantum Cryptography (QC), differentiating it from classical and even continuous-variable protocols. The study clarifies that QC achieves unconditional security based on quantum physical laws like the Heisenberg uncertainty principle and the no-cloning theorem, making eavesdropping detectable. They categorize Quantum Key Distribution (QKD) protocols into Discrete Variable (DV-QKD), like BB84 and B92, and Continuous Variable (CV-QKD), noting that DV-QKD is currently the more mature technology. The authors discuss key concepts of quantum information processing, including entanglement, measurement, and teleportation, which underpin these cryptographic protocols. They conclude that QC, especially QKD, is a vital technology for protecting future network communications against the threat of quantum computers.

[3] Durr-E-Shahwar, Imran, Altamimi, Khan, Hussain, and Alsaffar (2024), in their systematic literature review, establish QC as a necessary revolution for network security against quantum computational threats. They emphasize that traditional publickey cryptography (e.g., RSA, ECC) is fundamentally insecure against algorithms like Shor's, necessitating the transition to quantum-resistant schemes. The research clearly distinguishes QC (which relies on quantum mechanics for unconditional security in key exchange) from Post-Quantum Cryptography (PQC) (which relies on computational hardness against quantum attacks). The study documents numerous applications in secure communication, cloud computing, IoT security, and financial services, highlighting QC's potential to provide unparalleled and future-proof security. They conclude that despite challenges like cost and distance limitations, QC remains the most promising technology to ensure absolute confidentiality in the coming quantum .era.

[4] Li and Wang (2019) present an Optimized Coherent State Based Quantum Cryptography protocol focusing on achieving high robustness and long transmission distance, tackling known limitations of traditional CV-QKD. The core of their solution involves adopting a real local oscillator (LO) placed at the receiver (Bob) to circumvent side-channel attacks, and a discrete modulation strategy to enable operation at very low signal-to-noise ratios (SNR), crucial for long-range transmission. Through numerical simulations, they determine that discrete modulation with 4-state or 8-state schemes can offer advantages over Gaussian modulation for long distances. They acknowledge that real-world imperfections like phase mismatch, weak reference pulses (from the real LO), and modulator voltage fluctuation degrade performance, necessitating careful optimization.

[5] Rubio García, Cano Aguilera, Stan, Vegas Olmos, Rommel, and Monroy (2025) propose and demonstrate a triple-hybrid network security protocol that seamlessly combines Classical (e.g., ECDH), Post-Quantum (PQ) (e.g., ML-KEM-1024), and Quantum Key Distribution (QKD) into standard protocols like TLS 1.3 and IPsec (via RFC 9370). Their solution fundamentally addresses the "harvest now, decrypt later" (HNDL) attack threat by ensuring three independent cryptographic assumptions must be broken for the system to be compromised. The implementation uses a concatenation-based approach to combine the three shared secrets into a single key material (IKM) for the TLS key schedule. They show that while integrating real QKD equipment adds a performance overhead of about $57 ms (mainly due to key retrieval API latency), the solution is feasible and minimizes the packet overhead to only $36 for the QKD key ID.

IV. OBJECTIVE

- Establish Quantum-Resistant Security: Design and simulate a chat application that integrates quantum key distribution protocols to safeguard user communications against both classical and quantum attacks.
- Preserve User Privacy: Ensure that message content and metadata remain confidential, preventing unauthorized access or interception—even in scenarios involving adversaries with quantum computational capabilities.
- Demonstrate Protocol Feasibility: Assess the effectiveness and practicality of quantum cryptographic protocols within real-world messaging environments, focusing on performance, scalability, and usability.
- Evaluate System Robustness: Model and analyze resilience against channel noise, network losses, and potential side-channel threats, optimizing the system for secure and reliable message delivery.
- Promote Future-Proof Communications: Develop solutions and recommendations that enable the long-term adaptability of secure messaging platforms, anticipating emerging security challenges as quantum technology evolves.
- Support Practical Implementation: Provide simulation results, technical documentation, and guidelines to facilitate the integration of quantum-secure encryption

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

into existing communication infrastructures, benefiting developers and researchers

V. PROPOSED WORK

The proposed system is a secure chat application that uses the principles of Quantum Key Distribution (QKD) to make online messaging much safer. The main idea is to create and share secret keys between two users using quantum cryptography before they start chatting. This system uses the BB84 protocol in a simulated environment. Because of this, it removes many weaknesses found in normal encryption methods and strongly protects against eavesdropping and key theft.

The system is built with three main parts: User A's application, User B's application, and a Backend Server. Both users run the chat app on their own devices. Each user's app has four important modules. The first is a simple and friendly User Interface for typing and reading messages. The second is the Quantum Key Generation module, which simulates the BB84 protocol. It creates random quantum bits (qubits) and sends them to the other user. If someone tries to listen during this process, the quantum states get disturbed and the users can immediately detect it.

After the key exchange is completed safely, both users get the same secret key. This key is stored safely in the Key Store module on their devices. Then, the Encryption/Decryption module uses this key along with AES encryption to lock the messages before sending and unlock them after receiving. This ensures that only the two users can read the messages.

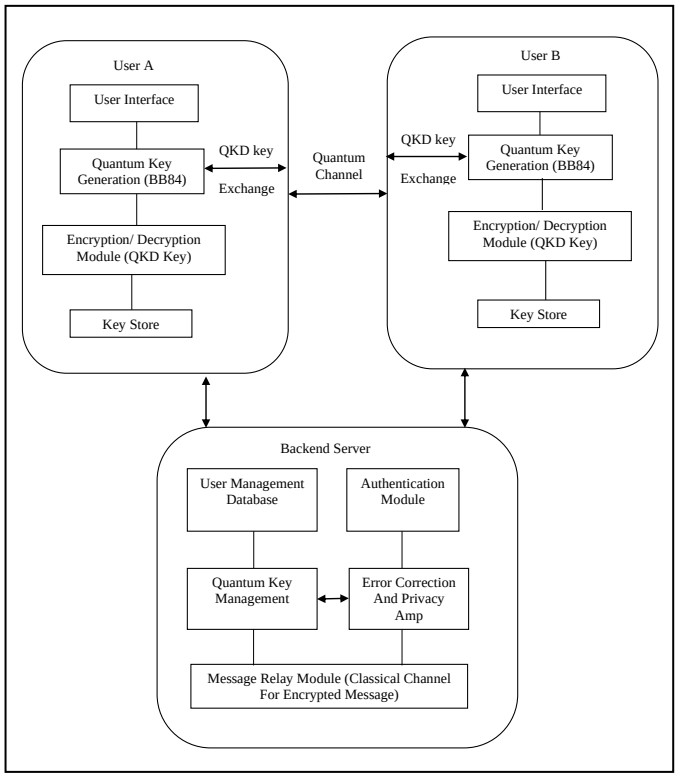
The Backend Server works as a helper in the middle. It does not see or store the secret keys, so it cannot read any messages. Its job is to manage user accounts, check login details through the Authentication Module, and deliver the encrypted messages between users. The server also helps with Error Correction and Privacy Amplification to remove mistakes and make the shared keys stronger and more secure.

This system has many advantages over regular chat applications. Traditional apps use mathematical methods like RSA that can be broken by future quantum computers. In contrast, this system uses the actual laws of quantum physics, which makes the key exchange much harder to break. Any eavesdropping attempt is quickly detected, and the messages stay fully private.

In summary, the proposed Secure Chat Application combines quantum cryptography simulation with normal chat features. It provides high security, strong privacy, and real-time messaging in a practical way. This project shows how quantum technology can be used today to build safer communication systems for the future.

VI. SYSTEM ARCHITECTURE

The proposed secure chat application follows a client-server architecture that combines quantum cryptography for key exchange with classical networking for message delivery. The system mainly consists of three parts: User A's application, User B's application, and a Backend Server. Both users have similar applications installed on their devices. Each user's app includes four important modules. The User Interface provides a simple chat screen for typing, sending, and reading messages. The Quantum Key Generation module simulates the BB84 protocol to create a shared secret key between the two users. These keys are exchanged through a simulated quantum channel. If anyone tries to eavesdrop during this exchange, the disturbance in the quantum states is immediately detected. Once the key is successfully generated, it is stored safely in the Key Store module on the user's device. The Encryption/Decryption module then uses this secret key with AES encryption to lock messages before sending and unlock them after receiving.



The Backend Server works as a supporting middle layer and plays an important role without compromising privacy. It never gets access to the secret encryption keys, ensuring that user conversations remain completely private. The server includes several key components. The User Management Database stores user profiles and credentials. The Authentication Module verifies users during login. The Quantum Key Management module helps coordinate the key exchange process between users. The Error Correction and Privacy Amplification module fixes any mistakes that occur during key exchange and removes weak bits to make the final key stronger and more secure. Finally, the Message Relay Module receives encrypted messages from one user and forwards them to the other user through a normal classical communication channel.

In this system, users first log in through the Backend Server for authentication. After logging in, when they start a chat, both users perform a simulated quantum key exchange using the BB84 protocol. Once they have the same secret key, all messages are encrypted using this key and sent through the Backend Server. The receiver then decrypts the message using the same shared key. This design provides strong end-to-end security because the server only relays encrypted messages and cannot read their content.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Overall, this architecture successfully combines the high security of quantum cryptography with the practical needs of real-time messaging. It offers better protection than traditional chat applications by making eavesdropping detectable and ensuring true privacy between users.

VII. WOKING PROCESS

The secure chat application works in a simple and step-by-step manner to provide safe communication between two users.

First, both users open the application and log in using their credentials. The Backend Server checks their login details through the Authentication Module and allows them to access the chat system.

Once logged in, when User A wants to chat with User B, the system starts the Quantum Key Exchange process. Both users' applications use the Quantum Key Generation module to simulate the BB84 protocol. They generate random quantum bits (qubits) and exchange them through a simulated quantum channel. During this exchange, if someone tries to eavesdrop, the disturbance in the quantum states is detected immediately. After checking for errors and making corrections, both users get the same secret key. This key is stored safely in their local Key Store.

After the secret key is successfully created, the actual chatting begins. When User A types and sends a message, the Encryption/Decryption module uses the shared secret key to encrypt the message. The encrypted message is then sent to the Backend Server through a normal internet connection. The Backend Server does not have the secret key, so it cannot read the message. It simply forwards the encrypted message to User B.

When User B receives the message, their Encryption/Decryption module uses the same shared secret key to decrypt it. User B can then read the original message. The same process happens when User B replies to User A. All messages are encrypted and decrypted only on the users' devices, ensuring complete privacy.

This entire process — quantum key generation, encryption, message relay, and decryption — continues throughout the chat session. The system also performs privacy amplification to make the key even more secure by removing any weak or leaked bits.

In short, the application first creates a highly secure shared key using quantum simulation, then uses that key to encrypt and decrypt all messages, while the server only helps in delivering the encrypted messages without ever seeing the content.

VIII. AES-256 ALGORITHM.

In the secure chat application, AES-256 is used as the main encryption method to protect the actual messages sent between users. AES stands for Advanced Encryption Standard, and AES-256 means it uses a 256-bit secret key — one of the strongest versions available today. While the BB84 quantum protocol is responsible for securely generating and sharing the secret key, AES-256 is used to actually encrypt and decrypt the chat messages.

After the two users successfully complete the quantum key exchange using the simulated BB84 protocol, they both possess the same secret key. This quantum-generated key is then fed into the AES-256 algorithm. When a user types a message, the Encryption module uses AES-256 to convert the plain text into unreadable encrypted data (called ciphertext) before sending it. On the receiver's side, the same AES-256 algorithm uses the identical secret key to convert the ciphertext back into the original readable message.

AES-256 works in multiple rounds of complex mathematical operations called substitution, permutation, and mixing. These operations scramble the data so thoroughly that it becomes extremely difficult for anyone to break, even with powerful computers. Because the key comes from the quantum simulation, it is highly random and secure, which further strengthens AES-256's protection.

The combination is very powerful: BB84 provides a secure way to share the key (with the ability to detect eavesdropping), while AES-256 delivers fast and highly secure encryption for the messages themselves. This ensures end-to-end encryption — meaning only the two users can read the messages. The Backend Server only relays the encrypted messages and never has access to the secret key.

Using AES-256 in this quantum cryptography simulation project offers several benefits. It is a well-tested, industry-standard algorithm that is fast enough for real-time chatting. It also provides forward secrecy — even if the key is somehow compromised later, previous messages remain safe. Most importantly, pairing a quantum-generated key with AES-256 creates a hybrid system that is resistant to both current cyber threats and future quantum computer attacks.

In short, AES-256 acts as the reliable workhorse that encrypts the actual chat content, while the quantum BB84 simulation ensures the key used by AES-256 is distributed in a highly secure and detectable manner.

IX. BB84 PROTOCOL

The BB84 protocol is one of the most well-known methods in Quantum Key Distribution (QKD). It was proposed in 1984 by Charles Bennett and Gilles Brassard. The main goal of this protocol is to allow two users, usually called Alice and Bob, to securely generate and share a secret key over an insecure communication channel. Unlike traditional encryption that depends on complex mathematics, BB84 uses the principles of quantum mechanics to create the key, making it possible to detect any attempt of eavesdropping.

In the BB84 protocol, information is sent using photons (particles of light) and their polarization states. There are two main measurement bases: the rectilinear basis (horizontal and vertical) and the diagonal basis (45° and 135°). Alice starts by generating a random sequence of bits (0s and 1s). For each bit, she randomly chooses one of the two bases and prepares a photon accordingly. She then sends these photons to Bob through a quantum channel.

When Bob receives the photons, he also randomly selects a basis to measure each one and records the result. After the transmission is complete, Alice and Bob use a normal classical communication channel to compare the bases they used for each photon. They only keep the bits where they both used the same basis. These matching bits form the raw key, while the mismatched ones are discarded.

To ensure the key is secure, Alice and Bob then check for errors by publicly comparing a small random portion of their

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

raw key. If the error rate is too high, they suspect that someone may have tried to intercept the photons and they discard the key. A few natural errors can occur due to noise, but too many errors indicate eavesdropping. After this, they perform error correction to fix any remaining mistakes so both have identical keys. Finally, they apply privacy amplification, which shortens the key to remove any possible information that an eavesdropper might have gained.

The biggest strength of the BB84 protocol is its ability to detect eavesdropping. According to quantum mechanics, measuring a photon disturbs its state. If an eavesdropper tries to measure the photons in between, it introduces detectable errors in the key. This allows Alice and Bob to know whether their communication is secure or not.

In this project, since real quantum hardware is not easily available, the BB84 protocol is fully simulated in software. The simulation follows all the important steps — random bit generation, basis selection, measurement, sifting, error checking, correction, and privacy amplification — to generate secure keys that are later used for encrypting messages in the chat application.

ACKNOWLEDGMENT

I would like to express my heartfelt gratitude to my project guide and mentors for their expert guidance, insightful suggestions, constant encouragement, and unwavering support throughout the entire duration of this project. Their valuable feedback and technical advice played a crucial role in overcoming challenges and successfully implementing the secure chat application using quantum cryptography simulation. I am sincerely thankful to my college and department for providing the necessary infrastructure, computing resources, and a conducive academic environment that enabled me to carry out this research work effectively. I am deeply grateful to my family members for their endless love, patience, motivation, and emotional support, which kept me focused and determined during difficult times. I also thank my friends and colleagues for their helpful discussions, constructive feedback, and constant encouragement. Finally, I acknowledge and appreciate the contributions of all researchers and scientists in the field of quantum cryptography and secure communication, whose pioneering work provided the strong foundation and inspiration for this project.

REFERANCES

[1] M. Li and T. Wang, “Optimized coherent state based quantum cryptography with high robust for networks deployment,” *IEEE Access*, vol. 7, pp. 109628–109634, 2019

[2] C. Rubio García, A. Cano Aguilera, C. Stan, J. J. V. Olmos, S. Rommel, and I. T. Monroy, “Enhanced network security protocols for the quantum era: combining classical and post-quantum cryptography, and quantum key distribution,” *IEEE J. Sel. Areas Commun.*, vol. 43, no. 8, pp. 2765–2781, 2025.

[3] A. M. A. Alnaser, H. M. S. Hatamleh, N. A. Almolhis, S. Duraibi, and Y. Alqahtani, “Secure quantum communication with multi-users in quantum networks,” *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2397–2417, 2025

[4] J. Li, N. Li, Y. Zhang, S. Wen, W. Du, W. Chen, and W. Ma, “A survey on quantum cryptography,” *Chin. J. Electron.*, vol. 27, no. 2, pp. 223–228, 2018

[5] S. Ricci, P. Dobias, L. Malina, J. Hajny, and P. Jedlicka, “Hybrid keys in practice: combining classical, quantum and post-quantum cryptography,” *IEEE Access*, vol. 12, pp. 23206–23219, 2024.

[6] F. Yang, D. Qiu, and P. Mateus, “Continuous-variable quantum secret sharing in fast-fluctuating channels,” *IEEE Trans. Quantum Eng.*, vol. 4, pp. 4100809-1–4100809-9, 2023].

[7] C. Lee, I. Sohn, and W. Lee, “Eavesdropping detection in BB84 quantum key distribution protocols,” *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 3, pp. 2689–2701, 2022.

[8] 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,” *J. Web Eng.*, vol. 23, no. 6, pp. 813–830, 2024.

[9] D.-E. Shahwar, M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar, “Quantum cryptography for future networks security: a systematic review,” *IEEE Access*, vol. 12, pp. 180048–180078, 2024.