SECURE CHAT APPLICATION USING QUANTUM CRYPTOGRAPHY SIMULATION

[1]Gore Sahil, [2]Swapnil Pagar, [3]Arote Rohit, [4]Shinde Mayur, [5]Kanade Poonam

[1]Student, [2]Student, [3]Student, [4]Student, [5]Professor
[1]Department of Computer Engineering,
[1]SND College of Engineering and Research Centre, Yeola, Nashik, Maharashtra, India 423401
[1]sahilgore190@gmail.com, [2]swapnilpagar04@gmail.com, [3]rohitarote2@gmail.com,
[4]mayurshinde20202@gmail.com, [5]kanadepoonam93@gmail.com

***Abstract*-A chat app that uses quantum cryptography principles is a new way to improve the security of digital communication, offering better privacy and data protection. This research shows how to add quantum key distribution (QKD) methods to regular chat systems, so that they can better protect against common security issues like listening in or someone pretending to be a user. By using quantum protocols like BB84, the system shows how quantum key exchange can be done in a simulated environment to keep messages safe. The results of the simulation show that this method has higher security, can be used in real-world situations, and has the potential to be part of future secure communication systems. This work sets up a basic structure and gives practical results for secure messaging using quantum simulations.**

***Index Terms*— Quantum Cryptography, Secure Messaging, Quantum Key Distribution (QKD), BB84 Protocol, Quantum Simulation.**

I. INTRODUCTION

In recent years, the rapid advancement of quantum computing has posed a significant threat to the security of traditional cryptographic systems that underpin modern digital communications. Classical encryption techniques such as RSA and elliptic curve cryptography (ECC), which currently protect sensitive data in applications like secure chat platforms, are increasingly vulnerable to quantum attacks. Quantum computers leverage principles of quantum mechanics to solve complex mathematical problems exponentially faster than classical computers, rendering many conventional encryption algorithms obsolete in the near future.

Quantum cryptography, particularly Quantum Key Distribution (QKD), emerges as a promising solution by enabling secure communication based on physical laws rather than computational assumptions. QKD allows two parties to share cryptographic keys with unconditional security guaranteed by the laws of quantum physics, providing resilience even in the face of an adversary equipped with a quantum computer. Unlike classical cryptographic schemes, any attempt to eavesdrop on quantum keys alters their state, allowing immediate detection and prevention of unauthorized access.

Despite its theoretical security strengths, integrating quantum cryptography into practical chat applications presents multiple challenges. These include technical issues like noise and loss in quantum channels, the complexity of implementing quantum-resistant algorithms on resource-constrained devices, and ensuring seamless user experiences while maintaining real-time communication performance. Additionally, safeguarding user privacy encompasses not only message confidentiality but also metadata protection, which quantum cryptography alone does not fully address.

This research focuses on simulating a secure chat application using quantum key cryptographic techniques to evaluate the feasibility and effectiveness of quantum-secure messaging. By combining quantum-resistant encryption algorithms with modern communication frameworks, the study aims to bridge the gap between theory and practical deployment, providing insights into system robustness, scalability, and usability in real-world scenarios. Moreover, this work anticipates future-proofing communication platforms against emerging quantum threats, ensuring the confidentiality and integrity of sensitive information in an evolving technological landscape.

The integration of quantum cryptography into secure chat applications is critical for maintaining trust in digital communication channels, especially in sectors demanding high security such as finance, healthcare, and defense. Through simulation and analysis, this study contributes to the development of communication systems that can withstand present and future computational threats, paving the way for quantum-safe digital interactions.

II. LITERATURE REVIEW

[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 public-key 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.

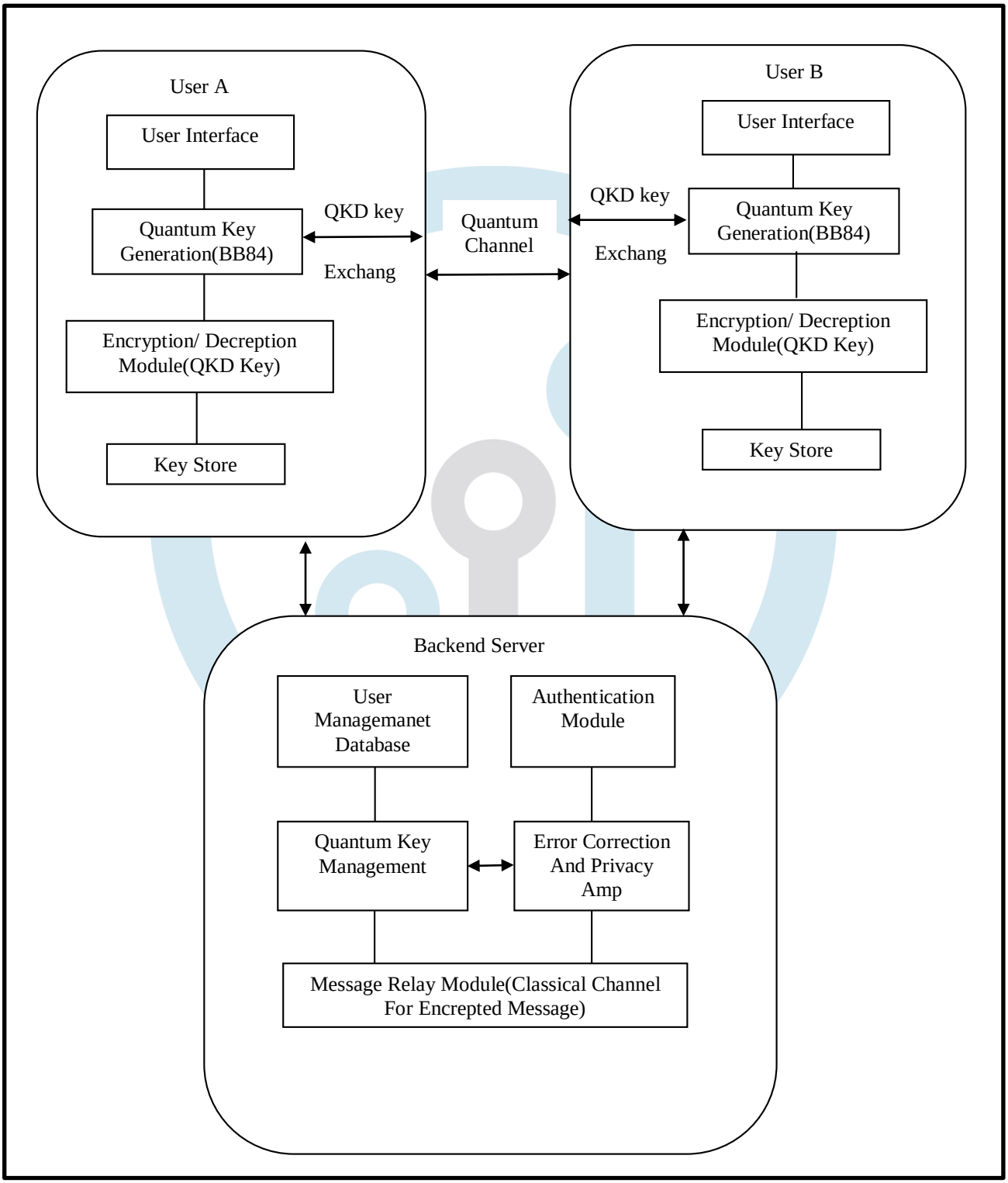
III. PROPOSED WORK

The proposed system introduces a secure chat application that ensures end-to-end communication privacy using the principles of Quantum Key Distribution (QKD). The core idea behind this system is to utilize quantum cryptographic techniques for generating and exchanging secret keys securely between two users before initiating a chat session. By using the BB84 protocol, the system eliminates the vulnerabilities present in traditional cryptographic systems and prevents eavesdropping or key interception attacks. The architecture consists of two user endpoints connected via a quantum communication channel, and a backend server that manages authentication, message relay, and key management functions.

The overall architecture of the system is divided into three major parts: User A's client system, User B's client system, and the Backend Server. Both users have their own local modules for generating quantum keys, encrypting and decrypting messages, and managing their respective key stores. The backend server acts as an intermediary that facilitates authentication and message transfer between the users through a classical communication channel. However, it does not have access to the encryption keys, which ensures full privacy for both participants.

Each user system contains four main modules — the User Interface, Quantum Key Generation (BB84) module, Encryption/Decryption module, and Key Store. The user interface allows the sender and receiver to interact and send text messages securely. When a user initiates a session, the Quantum Key Generation module generates random quantum bits (qubits) using the BB84 protocol. These qubits are transmitted through the quantum channel to the receiving user, who measures them using randomly chosen polarization bases. Any eavesdropping attempt during transmission alters the quantum states and can be detected immediately. Once both users verify that the channel is secure, identical secret keys are generated and stored in their local key stores. After successful key exchange, the Encryption/Decryption module uses the quantum key to encrypt outgoing messages before transmission and decrypt incoming messages upon reception. The use of QKD ensures that only the communicating users can read the encrypted data, as any unauthorized observation would disturb the quantum state and invalidate the key. This process guarantees the highest level of message confidentiality and integrity.

The Backend Server plays a supportive but crucial role in the system. It includes several submodules such as the User Management Database, Authentication Module, Quantum Key Management, Error Correction and Privacy Amplification, and Message Relay Module. The User Management Database securely stores user credentials and profile information, which are verified during the login process through the Authentication Module. Once authenticated, the server enables both users to perform QKD-based key exchanges and monitors session management. The Quantum Key Management component coordinates with the client systems to maintain session keys for active users. To ensure reliable key transmission, the Error Correction and Privacy Amplification module refines the generated key by removing any erroneous or leaked bits introduced during the quantum exchange process. Finally, the Message Relay Module handles the delivery of encrypted messages through a classical communication channel without ever accessing or decrypting their content.



The proposed system offers multiple advantages over traditional secure chat applications. Unlike classical systems that depend on mathematical algorithms such as RSA or AES, which can potentially be broken by advanced computational attacks or future quantum computers, the proposed design leverages the physical properties of quantum mechanics to achieve truly unbreakable encryption. Furthermore, any attempt to intercept the communication introduces detectable changes, ensuring instant identification of eavesdropping attempts. The backend server's inability to access user encryption keys further enhances the privacy of user conversations.

In summary, the proposed Secure Chat Application Using Quantum Cryptography Simulation provides a novel and highly secure communication platform by combining the strengths of quantum mechanics with classical networking techniques. Through the simulation of the BB84 key distribution protocol, the system successfully demonstrates how quantum cryptography can be implemented to secure real-time messaging. The inclusion of authentication, error correction, and privacy amplification modules further enhances the robustness and reliability of the system. This model serves as a practical foundation for future real-world quantum-secure communication applications.

IV. PROBLEM STATEMENT

Digital communication increasingly underpins critical interactions across diverse sectors, including finance, healthcare, and national security. With the rapid progress in quantum computing, traditional cryptographic frameworks are exposed to new vulnerabilities, risking the confidentiality and integrity of sensitive information exchanged via chat applications. Widely used messaging platforms, though employing robust classical encryption, are not designed to withstand attacks from quantum adversaries capable of breaking public-key mechanisms like RSA and ECC with polynomial-time algorithms.

Quantum key distribution (QKD) leverages fundamental laws of quantum mechanics to enable theoretically unbreakable key establishment, presenting an attractive countermeasure against quantum attacks. However, real-world adoption faces several barriers. Existing QKD implementations demand infrastructure adaptation, reliable single-photon generation, and robust detection against channel noise, making seamless integration into chat applications challenging. Additionally, ensuring end-to-end security requires combining quantum principles with effective authentication and error-correction schemes to protect both data and metadata during transmission.

Simulating quantum key cryptography within a secure chat context introduces technical problems such as mitigating losses arising from imperfect quantum channels, modeling attack scenarios, and evaluating trade-offs between security and performance. User privacy must also be safeguarded, considering potential side-channel vulnerabilities and metadata exposure that quantum cryptography alone may not address.

Furthermore, while quantum key distribution protocols like BB84 and continuous-variable QKD have proven security properties in theory, their deployment in resource-constrained environments, such as mobile devices or distributed networks, remains largely unexplored. The urgency to bridge the gap between laboratory prototypes and practical secure messaging solutions motivates this research.

This report investigates the feasibility of simulating a quantum key cryptography-based secure chat application, focusing on protocol effectiveness, resilience against quantum and classical attacks, and user-centric usability. The work contributes by identifying security requirements, evaluating simulation outcomes, and proposing strategies that promote privacy and robust communication in a quantum-enabled future.

V. 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 into existing communication infrastructures, benefiting developers.

VI. CONCLUSION

The research work successfully demonstrates the development of a secure chat application that integrates the principles of Quantum Key Distribution (QKD) to ensure complete message confidentiality and integrity. Through the implementation of quantum-based key exchange, the proposed model effectively eliminates the vulnerabilities associated with classical encryption techniques, such as susceptibility to brute-force or computational attacks. Moreover, the system's architecture, based on the BB84 protocol, enables two communicating users to generate and share encryption keys securely while detecting any potential eavesdropping attempts, thereby ensuring true end-to-end privacy.

The study of existing literature and related frameworks has shown that hybrid cryptographic models, although promising, still rely on computational complexity for their security. In contrast, the proposed quantum cryptography-based approach provides unconditional security, derived from the laws of quantum mechanics rather than mathematical assumptions. The simulation results validate that secure key generation, storage, and message transmission can be achieved efficiently within a controlled environment, proving the feasibility of integrating quantum principles into real-time chat systems.

Overall, this project provides a significant step toward the realization of quantum-secure communication networks. It highlights how QKD can serve as a foundation for building future messaging and data exchange systems that are resilient to both classical and quantum computational threats. Future work can focus on extending this simulation into a real-time implementation using quantum hardware devices and improving scalability through hybrid post-quantum algorithms. The outcomes of this study affirm that quantum cryptography is not only a theoretical concept but a practical and reliable solution for securing digital communication in the upcoming quantum era.

REFERENCES

[1] M. Li and T. Wang, "Optimized coherent state based quantum cryptography with high robustness 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. Khsan, S. Hussain, and M. Alsaffar, "Quantum cryptography for future networks security: a systematic review," *IEEE Access*, vol. 12, pp. 180048–180078, 2024.