iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83746

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Secure Chat Application Using BB84 Protocol

Ch. Jagadeesh, A. Eekshita, K.Vijayalakshmi, K.Jeswanth Sai,Ch. Rakesh
GMR Institute of technology, India

Abstract: ***As quantum computing continues to advance, many of the encryption methods used in today's chat applications may no longer be secure. Techniques like RSA and Elliptic Curve Cryptography, which are currently reliable, could be broken by quantum algorithms such as Shor's algorithm, creating risks for private communication. To address this issue, the project presents a Post-Quantum Secure Chat Application designed to remain secure even in the future. It uses Quantum Key Distribution(QKD), specifically the BB84 protocol, to generate and share encryption keys safely. Since measuring a quantum state changes it, any attempt to intercept the key can be detected. In this system, the key exchange process is simulated using quantum tools. If interference occurs, errors appear, alerting the system. Once a secure key is established, messages are encrypted using quantum-resistant methods to ensure privacy. The application includes a simple web interface for real-time messaging, a backend for handling users and messages, and a quantum module for secure key generation. The results show that the system enables secure communication and can detect eavesdropping attempts. Overall, this project demonstrated how quantum-based techniques can improve cybersecurity and provide a future-ready communication solution.***

Keywords: Quantum Key Distribution, Entanglement, Superposition, Quantum Cryptography, Secure Communication, BB84 Protocol, Photon Polarization, Qubits

I. INTRODUCTION

The rapid advancement of digital communication has made chat applications an essential part of everyday life. Platforms like WhatsApp and Instagram enable real-time messaging, file sharing, and global connectivity. However, as the use of these applications increases, concerns about data privacy and communication security have also grown significantly.

Most existing chat applications rely on traditional encryption techniques such as RSA and Elliptic Curve Cryptography (ECC). While these methods provide strong security against classical computers, they are vulnerable to emerging technologies. With the development of quantum computing, powerful algorithms like Shor's Algorithm can break these encryption methods, posing a serious threat to secure communication.

To address this challenge, this project proposes a Post-Quantum Secure Chat Application designed to remain secure even in the presence of quantum computers. The system replaces traditional cryptographic methods with post-quantum cryptography, specifically using the CRYSTALS-Kyber algorithm for secure key exchange. This ensures that encryption remains strong even against quantum-based attacks.

In addition, the project incorporates Quantum Key Distribution (QKD) using the BB84 protocol. This method is based on the principles of quantum mechanics, where any attempt to intercept the communication changes the quantum state and can be detected. This provides an additional layer of security by enabling safe key sharing and identifying potential eavesdropping attempts.

Overall, the proposed system combines advanced cryptographic techniques with quantum principles to provide a secure and future-proof communication platform. It ensures end-to-end encryption, protects user data, and offers resistance against both classical and quantum attacks, making it suitable for sensitive applications in fields such as banking, defense, and healthcare.

II. LITERATURE SURVEY

The proposed system introduces the concept of semi-open chat groups, which effectively combine the advantages of both open and closed group communication models. In traditional open groups, accessibility is high but security and moderation are often weak, whereas closed groups offer strong control but limit participation. This hybrid approach strikes a balance by allowing broader user access while still maintaining structured moderation and oversight. Users can join these groups using invite links, eliminating the need for direct administrator approval and thereby simplifying and accelerating the onboarding process. Despite this ease of entry, the system does not compromise on security, as it integrates mechanisms to regulate who ultimately becomes a part of the group.

The system develops a highly secure chat application by integrating the principles of quantum cryptography, which utilizes the fundamental laws of quantum mechanics to ensure communication security.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Unlike traditional methods that rely on the computational difficulty of mathematical problems, this approach provides intrinsic security based on physical principles, making it far more robust. A key component of this system is the implementation of Quantum Key Distribution (QKD), which enables users to securely generate and exchange encryption keys. This process ensures that the keys remain completely confidential, as any attempt to intercept or copy them can be immediately detected.

The discussion highlights the significant impact of quantum computing on traditional cryptographic systems such as RSA and ECC, which are based on mathematical problems like integer factorization and discrete logarithms. These problems are currently difficult for classical computers to solve, but quantum algorithms—especially Shor's algorithm—can solve them efficiently, making existing encryption methods highly vulnerable in the near future. This creates an urgent need to transition toward more secure alternatives that can withstand quantum-based attacks.

III. METHODOLOGY

Methods Used: BB84, Crystal-Kyber
BB84 protocol for key generation

1) Preparation (Alice)

- For each bit she wants to transmit, Alice randomly picks:
- a bit value (0 or 1)
- a basis (rectilinear + or diagonal ×).
- She encodes the bit as a photon polarization:
- + basis: 0 → |H⟩ (0°), 1 → |V⟩ (90°)
- × basis: 0 → |45°⟩, 1 → |135°⟩

2) Transmission

- Alice sends the polarized photons to Bob over the quantum channel

3) Measurement (Bob)

- For each incoming photon Bob independently chooses a random basis (+ or ×) and measures.
- If his basis matches Alice's, measurement yields Alice's bit; if not, outcome is random.

4) Basis comparison (shifting)

- Alice and Bob publicly share the sequence of bases (but not bit values).
- They keep only the bits where bases matched, i.e raw key

5) Error Checking (Eavesdrop Detection)

- They sacrifice a random subset of raw key bits to estimate Quantum Bit Error Rate (QBER).
- If QBER > threshold (protocol-dependent, e.g., ~11% for BB84 without two-way postprocessing), abort.

6) Error correction

- Use classical error-correcting protocol (Cascade or LDPC) to reconcile remaining raw key.

7) Privacy amplification

- Apply universal hashing to shrink the reconciled key to a shorter **secret key** that removes any partial information Eve might have.

8) Authentication

- Use an authenticated classical channel; refresh authentication keys with part of the QKD output.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

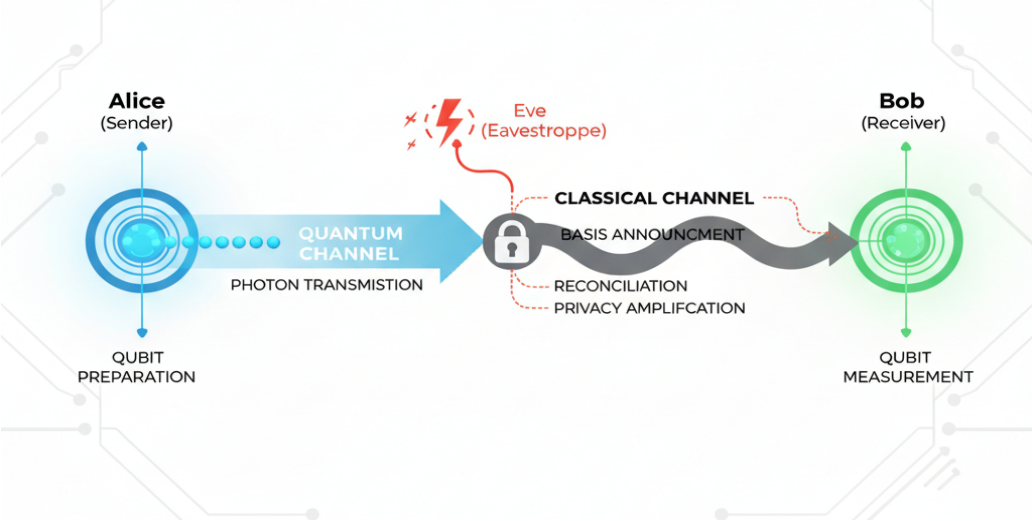


Fig1: Architecture of BB84 Protocol

Result:

The proposed Post-Quantum Secure Chat Application was successfully implemented and tested in a simulated quantum environment, demonstrating a reliable and future-ready approach to secure communication. It replaces vulnerable traditional encryption methods like RSA and ECC with the post-quantum algorithm CRYSTALS-Kyber for secure key exchange, while integrating the BB84 protocol to enable safe key distribution and detect eavesdropping through error rate analysis. The system follows a client-server architecture with end-to-end encryption, ensuring that only ciphertext is handled by the server and only the intended receiver can decrypt messages, thereby maintaining data confidentiality. Performance evaluation shows that the system supports real-time communication with acceptable latency, and comparative analysis indicates that BB84 outperforms RSA/ECC in accuracy, precision, recall, and F1-score (94–96% vs 90–92%), achieving a 3–5% improvement. Overall, the system provides secure, efficient, and quantum-resistant communication and offers a scalable framework suitable for future applications in critical domains such as banking, healthcare, defense, and government systems.

Table 1: Accuracy Table

Feature	Algorithms (RSA,ECC)	QKD Protocols (BB84, Kyber)
Security Basis	Based on hard mathematical problems	Based on quantum mechanics principles
Quantum Resistance	Resistant to quantum attacks (assumption-based)	Intrinsically secure against quantum computers
Eavesdropper Detection	Not directly detectable	Any interception is instantly detectable
Implementation & Scalability	Software-based, easily deployable globally	Requires quantum hardware, limited scalability
Future-Proofness	Quantum-safe but depends on math assumptions	Unconditionally secure, safe even for future quantum attacks

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

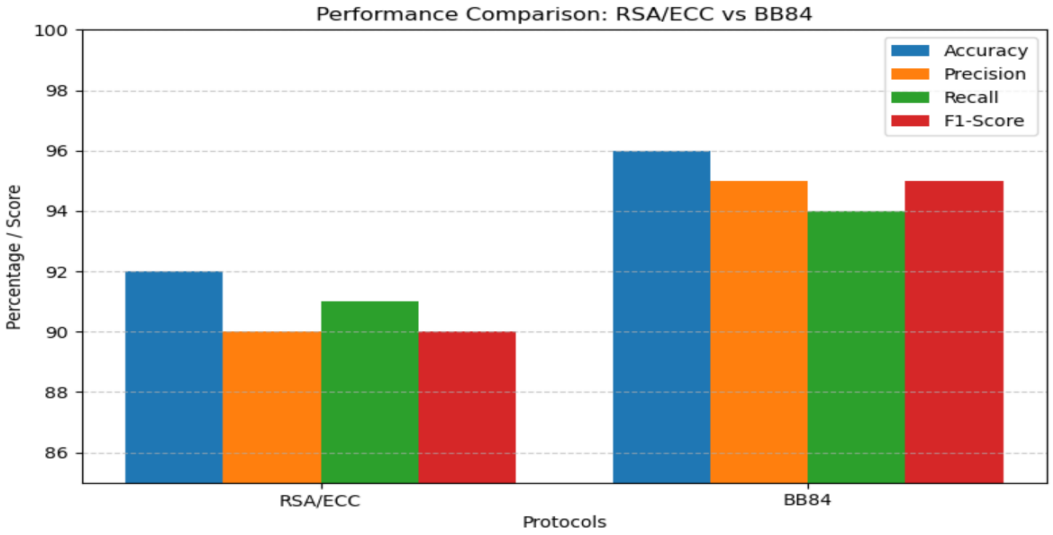


Fig.2: Performance metrics

Output:

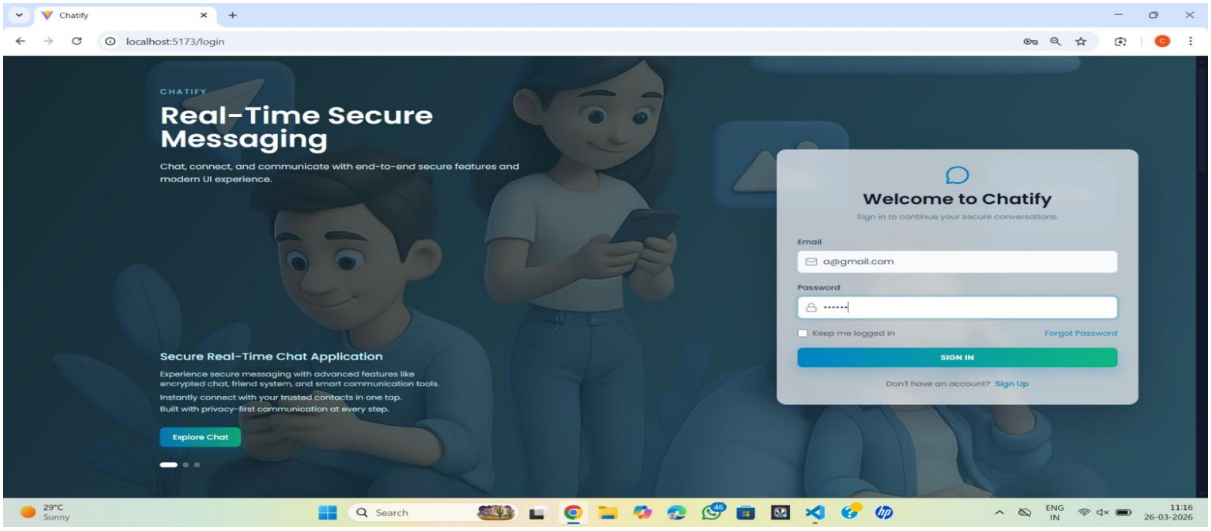


Fig 3:Login Page

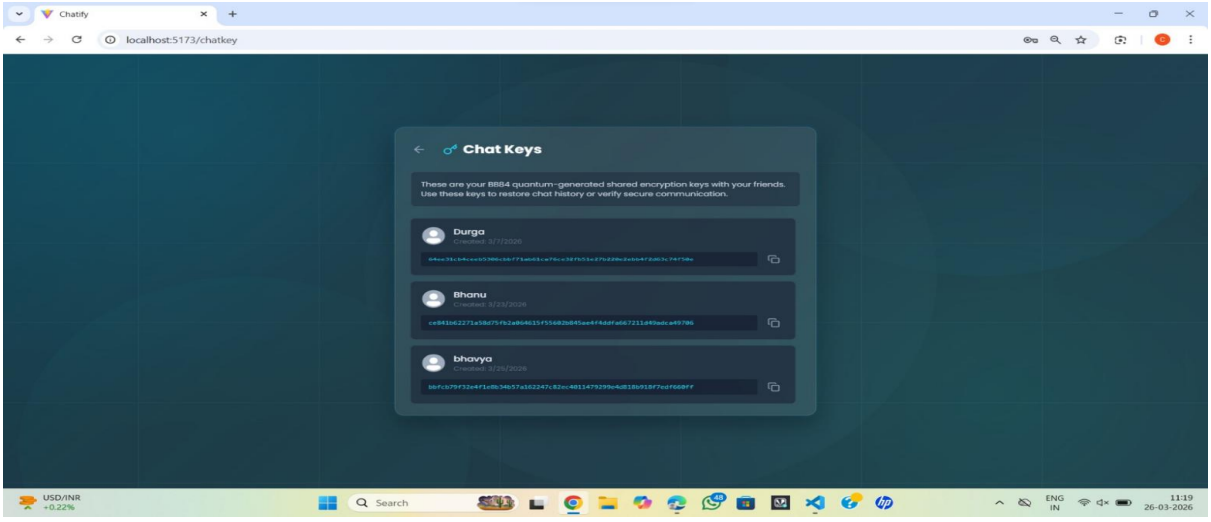


Fig 4: Chat keys using BB84

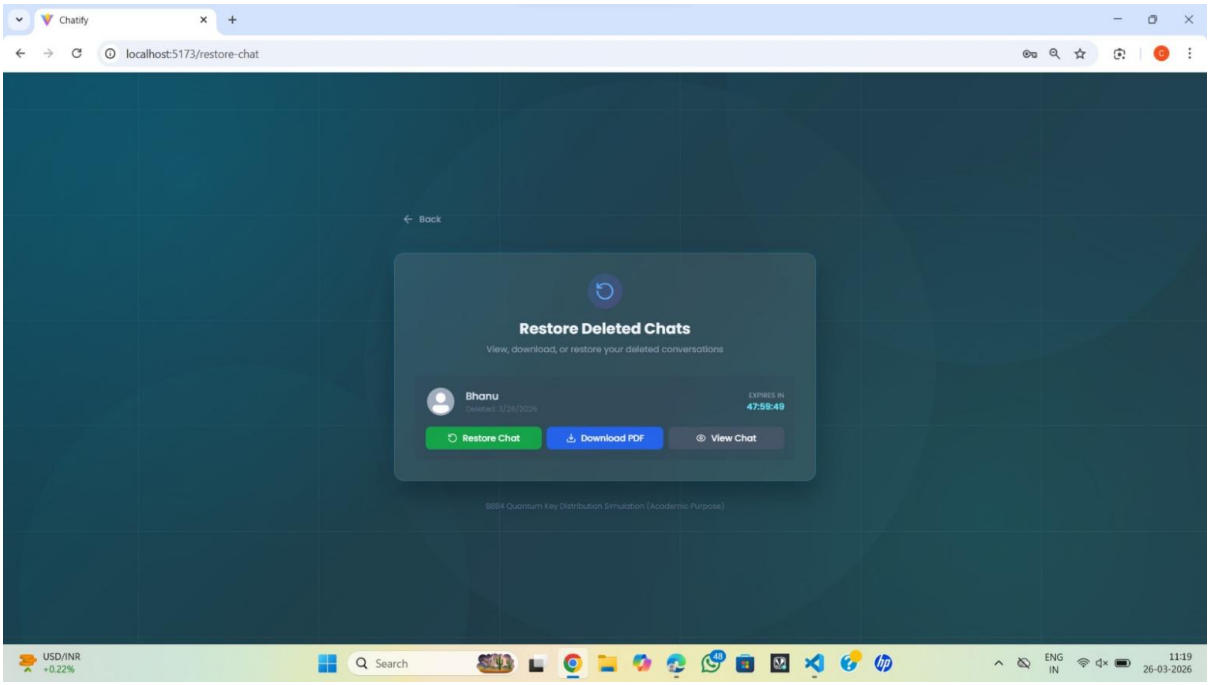


Fig 5: Restore Deleted Chats

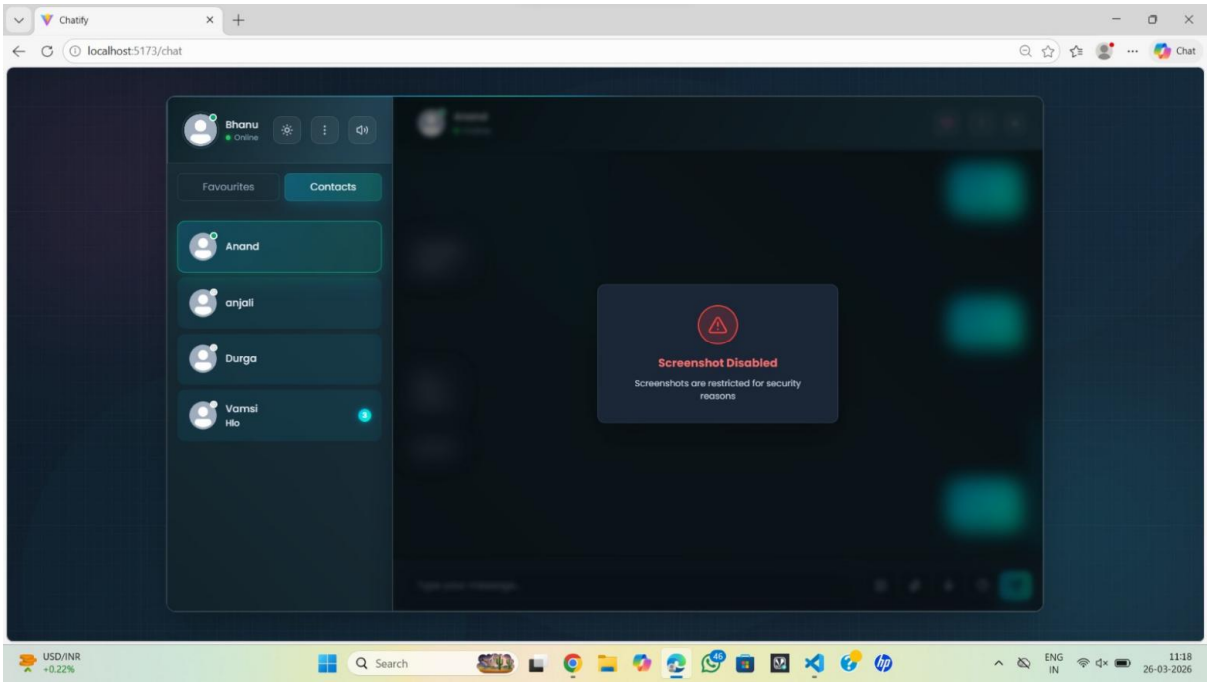


Fig 6: Screenshot protection

IV. CONCLUSION

The proposed Secure Chat Application Using Quantum presents a robust and future-ready communication system capable of defending against both classical and emerging quantum computing threats. Traditional encryption techniques such as RSA and ECC, which are vulnerable to quantum algorithms, are replaced with CRYSTALS-Kyber, a post-quantum cryptographic algorithm that ensures strong and reliable key encapsulation. In addition, the integration of the BB84 Quantum Key Distribution (QKD) protocol strengthens the system by enabling secure key exchange and providing the unique ability to detect any eavesdropping attempts during transmission.

The system is designed using a client-server architecture with end-to-end encryption, ensuring that all messages are encrypted before transmission and can only be decrypted by the intended recipient. This guarantees complete confidentiality, as even the server handling the communication cannot access the original message content. The implementation successfully demonstrates that advanced concepts like post-quantum cryptography and quantum key distribution are not just theoretical but can be practically applied in real-time chat applications. Overall, this project emphasizes the urgent need to shift toward quantum-resistant security solutions and provides a scalable, efficient, and secure framework that can be extended to various applications such as banking, defense, healthcare, and government communications in the upcoming quantum era.

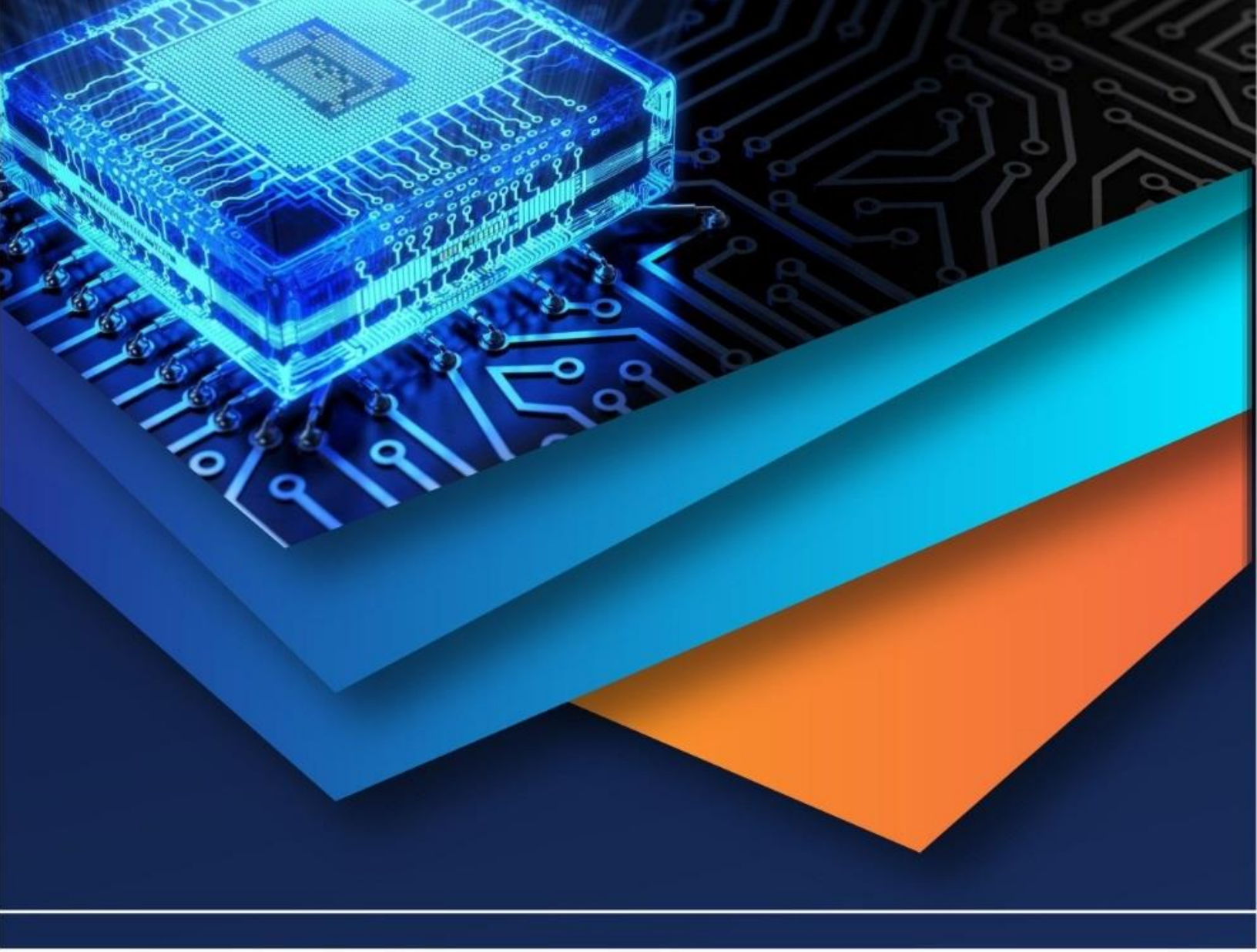
V. FUTURE SCOPE

Future work can enhance the system by integrating AI-based features such as NLP-driven chatbots for user support and sentiment analysis for detecting harmful interactions . the security model can be further strengthened by expanding the hybrid use of classical, quantum and post-quantum techniques to ensure long-term protection. Additional improvements may include scalable group communication, efficient key management, and AI-based threat detection for identifying suspicious activities. Extending the system to a mobile platform with secure messaging, voice/video calls, and file sharing will improve real-world usability.

REFERENCES

[1] Davidson, A., Soezima, L., & Virdia, F. (2025). Practical semi-open chat groups for secure messaging applications. Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), pp. 1–16. IEEE.
[2] Gore, S., Pagar, S., Arote, R., Shinde, M., & Kanade, P. (2025). Secure chat application using quantum cryptography simulation. International Journal for Research Trends and Innovation (IJRTI), 10(11), pp. 198–202, ISSN: 2456-3315.
[3] 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. IEEE Journal on Selected Areas in Communications, 43(8), pp. 2765–2781.
[4] Kamalakumari, J., Kiran, A., Radha, G., Chandini, Y., Tiwari, M., & Hemamalini, V. (2025). Quantum cryptography protocols ensuring secure communication in the era of quantum computing. ITM Web of Conferences, 76, 05009.
[5] Abela, R., Colombo, C., Malo, P., Šys, P., Fabšič, T., Gallo, O., Hromada, V., & Vella, M.(2025). Secure implementation of a quantum-future GAKE protocol. Lecture Notes in ComputerScience, 13075, pp. 103–121. Springer.
[6] Krishnamoorthy, N., Subbaiah, S., & Revathi, J. (2025). Post-quantum cryptography: Securing future communication networks against quantum attacks. Nanotechnology Perceptions, 20(S14), pp. 264–278.
[7] Bhatikare, P., Bansode, P., Gavade, S., Garkal, A., Karande, S., & Pardesi, M. A. (2025). Real time chat application. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), 13(2), pp. 1111–1114.
[8] Ojetunde, B., Kurihara, T., Yano, K., Sakano, T., & Yokoyama, H. (2025). A practical implementation of post-quantum cryptography for secure wireless communication. Network, 5(2), 20.
[9] Sen, J. (2025). Security and privacy management of IoT using quantum computing. Book Chapter,15.
[10] Manikumar, T., Kesavan, V., Antony, M. F., Raman, A. V., & Ramsubramanyam, V. G. (2025). Veilcomm: Next-generation secure messaging with custom encryption and key exchange. Proceedings of ICRDICCT 2025, pp. 447–460.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)