Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

QuMail: A Quantum-Resilient Secure Email Framework Integrating QKD Simulation, Post-Quantum Cryptography, and Blockchain Logging

Mohammad Reehan Nawaz
School of Computer Science Engineering
Presidency University
Bengaluru, India

Mohammad Afaque
School of Computer Science Engineering
Presidency University
Bengaluru, India

Anzer Hussain
School of Computer Science Engineering
Presidency University
Bengaluru, India

Dr. Anand Prakash
Associate Professor
School of Computer Science and Engineering Presidency University,
Bengaluru, India

***Abstract*—The emergence of quantum computing poses a significant threat to classical cryptographic mechanisms such as RSA and Elliptic Curve Cryptography that are widely used to secure email communication. Traditional secure email systems rely on classical public-key infrastructure and therefore lack resilience against quantum attacks. This paper presents QuMail, a quantum-secure email client that integrates BB84-based Quantum Key Distribution (QKD) simulation, CRYSTALS-Kyber post-quantum cryptography (PQC), and blockchain-based audit logging within a unified architecture. The proposed system operates entirely at the application layer and remains compatible with existing email infrastructures using standard SMTP and IMAP protocols without requiring any server-side modification. A modular prototype was implemented using IBM Qiskit for quantum key generation and hybrid cryptographic techniques for secure message transmission. Experimental evaluation demonstrates an average latency of 120–180 ms for QKD key generation and 20–30 ms for Kyber-based encryption while maintaining minimal overhead for email transmission. The results demonstrate the feasibility of integrating quantum-resilient security mechanisms into existing email systems and highlight the potential of hybrid QKD–PQC architectures for next-generation secure communication platforms.**

***Index Terms*—Quantum Key Distribution, Post-Quantum Cryptography, Secure Email, CRYSTALS-Kyber, Blockchain Audit Log, Qiskit, Quantum-Safe Communication**

I. Introduction

Email remains a fundamental form of communication for individuals and organizations alike. But as quantum computing advances at a rapid pace, traditional cryptographic systems like RSA and elliptic curve cipher, may be put into serious danger due to algorithms like Shor's algorithm [11]. This has led to an increasing demand for communication systems resistant to quantum-based attacks.

Quantum Key Distribution (QKD) allows two communicating parties to generate shared secret keys based on the well-founded properties of quantum mechanics including superposition and measurement disturbance [1], [17]. Simultaneously, Post-Quantum Cryptography (PQC) works towards the construction of classical cryptographic algorithms which are secure against quantum adversaries [12], [13]. While potentially beneficial, these techniques present practical challenges when implemented into existing email infrastructures since they have to comply with current communication protocols.

We introduced QuMail, a quantum-secure email client that leverages QKD to generate keys while using post-quantum encryption through the CRYSTALS-Kyber (Kyber) algorithm to secure emails. The system operates at the application layer and remains compatible with standard SMTP/IMAP servers such as Gmail and Yahoo without requiring server-side modifications.

Current email security solutions (e.g. Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME)) are built on well-established public-key cryptographic protocols like RSA and elliptic curve cryptography [10], [23]. While these methods protect us robustly now, they are technically endangered in the long run given advances in quantum computing. Transport Layer Security (TLS) secures data in transit, but is not able to guarantee long-term confidentiality for stored or intercepted data.

In the last few years, research has focused on leveraging work done in both QKD and PQC to create systems that are resistant to quantum attacks. At the same time, future communication infrastructures will likely integrate quantum-safe networking technologies alongside theoretical frameworks like

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

the quantum internet [20]. Yet, most of these methodologies are at the network level and not an application-layer like a secured email systems.

Therefore, there remains a significant research gap in designing practical quantum-resilient email systems that can operate on current SMTP/IMAP infrastructure without requiring modifications to existing mail servers. Several studies have explored quantum-safe cryptography, secure communication systems, and quantum networking architectures [2]–[7], [9], [15], [18], [21], [22], [25]–[28].

Increased QCA developments are driving rapidly the need for next-generation security solutions. Because quantum algorithms could break many of the most widely used public-key systems, there is an interest in exploring alternative approaches to cryptography. Well, QKD is a mathematically secure key exchange mechanism while PQC provides practical constructions feasible on classical networks. Combining these approaches gives solid building blocks for quantum-resilient communication systems.

Post-Quantum Cryptography introduces several mathematical approaches designed to resist quantum attacks, including lattice-based, code-based, and hash-based techniques [12], [13]. Among these, CRYSTALS-Kyber has been selected by NIST as a standard for secure key encapsulation due to its strong security guarantees and efficient implementation [3], [9]. Indeed, integrating such algorithms into real-world systems allows us to deploy quantum-safe solutions for communications at last.

Although quantum and post-quantum cryptography has made enormous progress since its first introduction, it still lacks a prominent presence in popular applications like email clients. Most existing work is either theoretical models or tailored infrastructure. Hence, it is necessary to implement application-layer systems that can embed quantum-safe mechanisms in existing communication environments. QuMail fills this gap by providing a unified theoreti- cal framework for QKD simulation, PQC and logging based on blockchain.

The remainder of this paper is organized as follows. Section II presents a detailed review of existing research in quantum cryptography, post-quantum cryptographic systems, secure email communication protocols, and blockchain-based communication logging. Section III describes the proposed QuMail system architecture and methodology. Section IV presents the implementation details and user interface components of the system. Section V explains the Quantum Key Manager module and BB84-based QKD simulation. Section VI describes the blockchain-based audit logging mechanism. Section VII explains the end-to-end security workflow of the system. Section VIII presents the experimental results and performance evaluation. Finally, Section IX concludes the paper and outlines future research directions.

II. Related Work

A. Quantum Cryptography and QKD

Quantum Key Distribution (QKD) is a long-known protocol for secure key exchange based on the fundamental principles of quantum mechanics. BB84 and similar protocols let two people create a shared secret key while detecting any wiretap attempts by measureable disturbances to the quantum states [1]. While QKD has been successfully demonstrated in optical fiber and satellite-based systems [16], [19], its widespread adoption is limited by reliance on specialized hardware and infrastructure.

B. Post-Quantum Cryptography

Its main goal is the designing of suitable encryption algorithms that are secure even in the face both classical and quantum adversaries. Lattice-based, code-based and multivariate [12], [13]are among different proposed approaches to achieving this goal. One example of such a post-quantum standard is CRYSTALS-Kyber which is lattice-based and has been included by NIST in its set of standards due to its ideal ratio between high security level and computational efficiency [3], [9].

C. Secure Email Communication

Traditionally, various forms of email security have relied upon standards like Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) [10]. Aimed at providing confidentiality and user authentication [23], these approaches rely on standard public-key encryption methods such as RSA and Diffie–Hellman algorithms. Finally, Transport Layer Security (TLS) is commonly deployed to encrypt communication channels between mail servers in transit [25]. Yet, these security mechanisms rely on mathematical problems that are rendered insecure when one implements quantum computing. Consequently, the increased interest in applying quantum-resilient methods of cryptography to provide long-term sustainability for email systems has arisen.

D. Blockchain for Secure Communication

Blockchain technology has become a promising approach for ensuring tamper-resistant records and establishing decentralized trust in distributed systems. It works by maintaining a continuously growing ledger of transactions, where each record is securely connected using cryptographic hash links and validated through consensus mechanisms [14]. Because of these characteristics, blockchain can be effectively used for securely logging communication activities and cryptographic processes. Earlier research has examined the use of blockchain-based audit systems in areas such as secure communication networks, identity management, and distributed trust frameworks [27], [28]. When blockchain logging is integrated with secure communication platforms, it can enhance transparency, improve traceability, and support reliable forensic analysis of communication events.

E. Hybrid Quantum-Secure Communication Systems

Recent studies have investigated hybrid security models that combine quantum cryptographic methods with traditional communication systems to enable practical implementation of quantum-resistant security solutions. In these architectures,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

Quantum Key Distribution (QKD) is typically used to generate secure cryptographic keys, while conventional communication channels are still used to transmit the encrypted data.

A number of research efforts have focused on combining QKD with post-quantum cryptographic algorithms to improve the overall security of distributed communication networks. These hybrid systems aim to merge the strong theoretical security offered by quantum cryptography with the practicality and flexibility of classical cryptographic techniques.

In addition, researchers have proposed quantum-secure messaging frameworks that utilize post-quantum encryption methods such as CRYSTALS-Kyber for key encapsulation while ensuring compatibility with current internet communication protocols. Such designs show that it is possible to build communication systems that remain secure in the era of quantum computing without requiring significant changes to existing network infrastructure.

Despite these developments, many of the proposed solutions mainly target network-level protocols or specialized communication systems rather than applications used directly by end users. Therefore, there is still a clear need for practical quantum-secure solutions that can function within commonly used application-layer platforms, including email clients.

F. Research Gap

Although significant research has been carried out in areas such as quantum cryptography, post-quantum cryptography, and blockchain-based security, most studies tend to examine these technologies separately. Only a limited number of works have explored how these approaches can be combined, particularly within practical application-layer systems like email clients. In particular, the integration of QKD simulation, post-quantum encryption, and blockchain-based logging in a single framework has not been widely addressed. To bridge this gap, this research introduces the QuMail framework, which integrates these technologies into a unified architecture to enable quantum-resilient email communication without requiring modifications to the existing email infrastructure.

III. Proposed System Architecture and Methodology

The QuMail architecture is layered and modular in nature, allowing it to fit alongside the existing email ecosystem while supporting better security mechanisms as they become available. Since the system operates at the application layer, it does not require modifications to external SMTP or IMAP servers.

The architecture consists of the following functional components:

- **User Interface Layer** – Supplies a dashboard for drafting, viewing, decrypting and auditing emails. It also shows the key generation and security status.
- **Security Policy Manager** – When a user selects one of the security levels, this component decides which encryption protocol to use and enforces key usage policies.
- **Encryption Engine** – Hybrid encryption (RSA-2048/AES-256), post-quantum key encapsulation via CRYSTALS-Kyber, OTP via QKD-derived One-Time Pad (OTP) or else AES session keys.
- **Quantum Key Manager** – Produces random symmetric keys with high entropy through a BB84 design QKD simulation using IBM Qiskit. It carries out qubit preparation, basis selection, measurement and key reconciliation.
- **Secure Local Key Cache** – Keeps generated quantum keys and PQC session keys in encrypted format, extending the single-instance condition for OTP operations.
- **Email Protocol Handler** – Handles SMTP for sending messages, IMAP retrieves them, and MIME encodes/decodes an encrypted payload.
- **Blockchain Audit Logger** – Allows the logging of cryptographic events such as key generation, encryption and decryption into a tamper-evident log structured by hash-linking to provide non-repudiation.

A. Data Flow

Upon sending a message, the user composes an email and chooses a level of security. The Security Policy Manager calls the appropriate cryptographic module in the Encryption Engine. In case of choosing QKD mode, the Encryption Engine requests a key with its key identifier from the Quantum Key Manager. It encrypts the payload locally, wraps it as a MIME attachment, and sends it via the SMTP client over TLS.

On the receiver side, the IMAP client receives the encrypted mail. The security metadata is extracted, the corresponding key (if it exists) is fetched from the local cache, integrity verification is performed and the payload is decrypted for display in the inbox preview panel.

B. Key Management Workflow

The quantum keys generated by the QKD simulator are deposited in a secure cache with essential metadata, including key ID, length and current usage state. (IV) OTP mode cannot be repeated (keys are immediately invalidated), providing perfect secrecy. The architecture is also extendable to support ETSI GS QKD 014–compliant REST interfaces for integration with hardware QKD systems in the future.

C. Security and Interoperability

All encryption operations are performed at the application layer right before being transmitted via SMTP, retaining ciphertext on a public network. While the transport-layer TLS is kept to protect each channel, offering a hybrid security model. By implementing standard SMTP/IMAP protocols, it is interoperable with existing email providers like Gmail and Yahoo.

The blockchain module operates independently from the encryption workflow and logs only hashed transaction metadata, not plaintext content, so it maintains confidentiality yet enables forensic traceability.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

D. Secure Email Transmission Algorithm

Algorithm 1 outlines the secure transmission workflow implemented in the QuMail system. The algorithm describes the steps involved in encrypting and transmitting a secure email using the selected security mechanism.

Algorithm 1: QuMail Secure Transmission

Input: Message M

Output: Encrypted email payload C

1) User composes message M
2) Generate symmetric session key K_s
3) If security level = PQC
   - Encapsulate K_s using CRYSTALS-Kyber
4) Else if security level = QKD
   - Retrieve one-time key from QKD Key Manager
5) Encrypt message using AES-256
6) Create blockchain transaction entry
7) Encode encrypted payload using MIME
8) Send encrypted email via SMTP over TLS

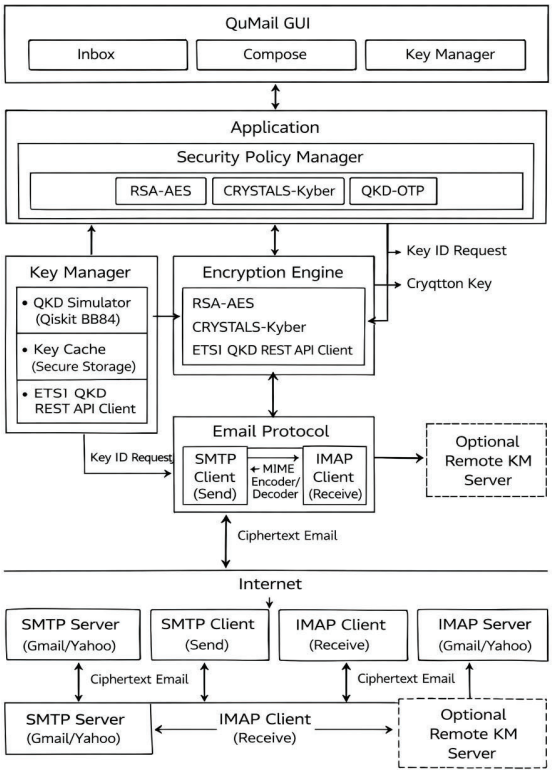

Fig. 1. QuMail system architecture integrating QKD key manager, encryption engine, SMTP/IMAP interface, and blockchain audit module.

IV. System Implementation

The QuMail prototype was developed in the form of a Windows desktop application with a modular and security-focused dashboard. The interface provides real-time visibility into key management, encryption status, and audit logging through a simple abstraction over complex cryptographic operations.

A. Login Interface

The login module provides authentication between the user and external email servers. Users enter the email address of their Gmail/Yahoo account as well as an application password. After submission, the client sets up secure IMAP and SMTP sessions using TLS encryption. When authentication is successful, the local key cache is initialized and Quantum Key Manager gets enabled.

Session tokens are short lived, existing only until the end of an active session and removed on logout to prevent further unauthorized use. This allows communication channels and cryptographic operations to be initiated from within a trusted environment.

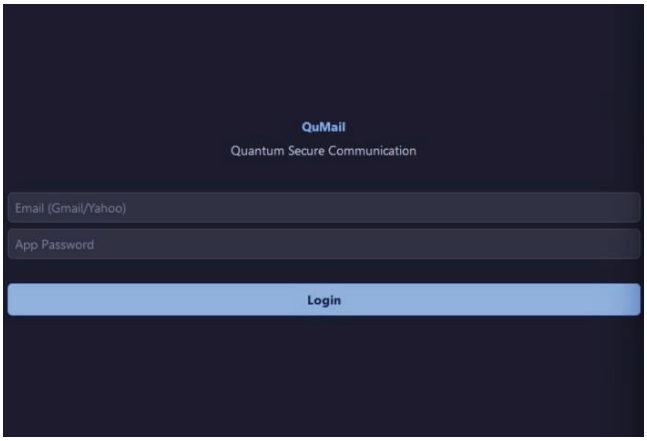

Fig. 2. Login interface for secure authentication with external email servers.

B. Secure Reception Module (Inbox)

The inbox module receives incoming emails and classifies them for decryption. It utilizes a dual-pane structure that arranges the synchronized message list with a preview panel. IMAP is used to retrieve emails, while MIME decoding is used to parse encrypted message payloads.

When your messaging app gets an encrypted message (like one protected with AES), it uses the extra security info sent with it to figure out how strong the encryption is. It retrieves the corresponding key from local key cache using this key identifier. Integrity verification is performed using authenticated encryption (AES-GCM tag validation) before decrypting.

A quantum security report is displayed to the user, indicating:

- Encryption protocol used (RSA-AES, Kyber, or QKD-OTP)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

- Key retrieval status
- Ciphertext payload received over the public network
- Successfully decrypted plaintext message

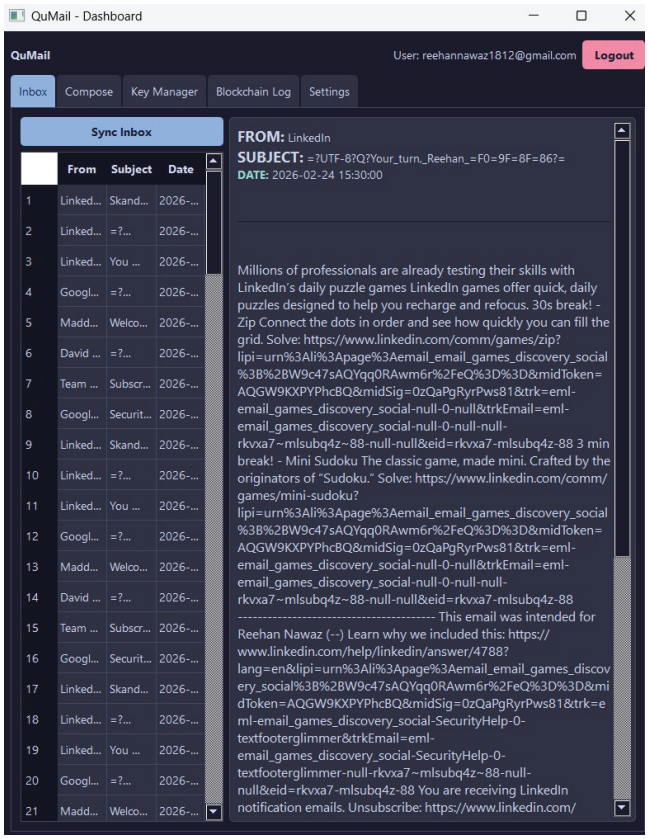

Fig. 3. Secure inbox with dual-pane decryption view.

C. Secure Transmission Module (Compose)

The compose module is responsible for the email encryption for outgoing emails. They fill in the recipient address, subject and message body, then pick a desired security level from a multi-layer cryptographic menu.

Based on the selected level, the system performs:

- Public key retrieval (RSA or Kyber)
- Quantum key acquisition from the Key Manager (for QKD mode)
- Session key generation and payload encryption
- MIME encapsulation of the encrypted message

Attachments are encrypted under the same session key for uniform confidentiality. The mail server can now deliver the encrypted payload via SMTP-over-TLS to any external mail server without modifying this external mail server.

V. Quantum Key Manager

The BB84 protocol represents quantum bits (qubits) [1] using orthogonal and diagonal basis states:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

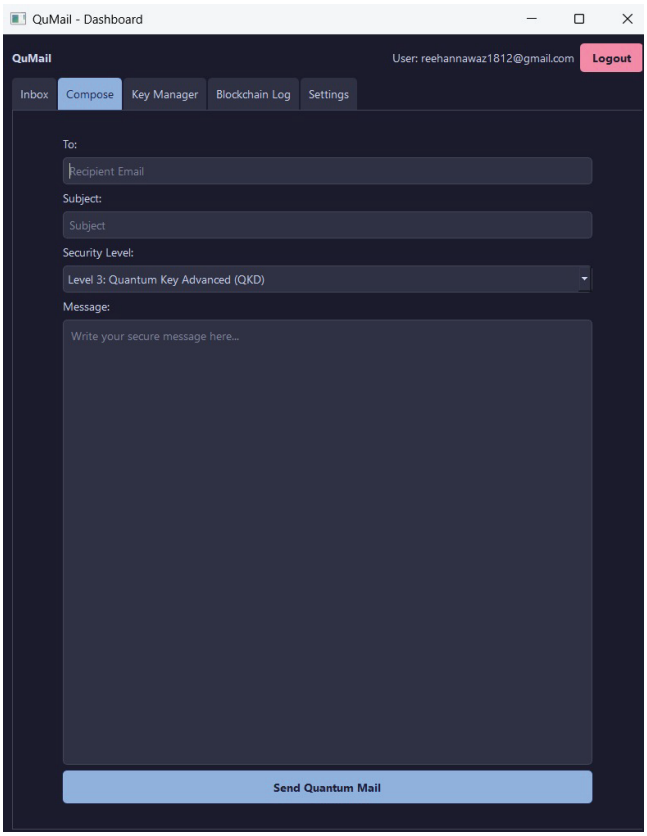

Fig. 4. Compose module with multi-level encryption selector.

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

The result you get when measuring a quantum state depends on how probable that state is

$$P = |\langle\psi|\phi\rangle|^2$$

where ψ represents the transmitted qubit state and ϕ represents the measurement basis.

The Quantum Key Manager provides a simulation of BB84-based Quantum Key Distribution using the IBM Qiskit framework. Quantum computation principles underlying such protocols are widely described in foundational literature [24]. The module produces high-entropy symmetric keys by putting qubits in superposition with Hadamard gates and then measuring the qubits in randomly selected bases.

The raw key, which is generated, is then reconciled over the basis and filtered to obtain a common secret key. Although implemented as a simulation, the workflow reflects operational QKD systems [16], [19].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

The interface shows live logs of qubit preparation, basis selection, measurement results and final key generation. Keys generated are cached securely on local store and marked for single use in OTP mode preventing keys reuse while its properties exhibit perfect secrecy.

The Key Manager also features ETSI GS QKD 014– style REST API integration for future hardware QKD device interfacing.

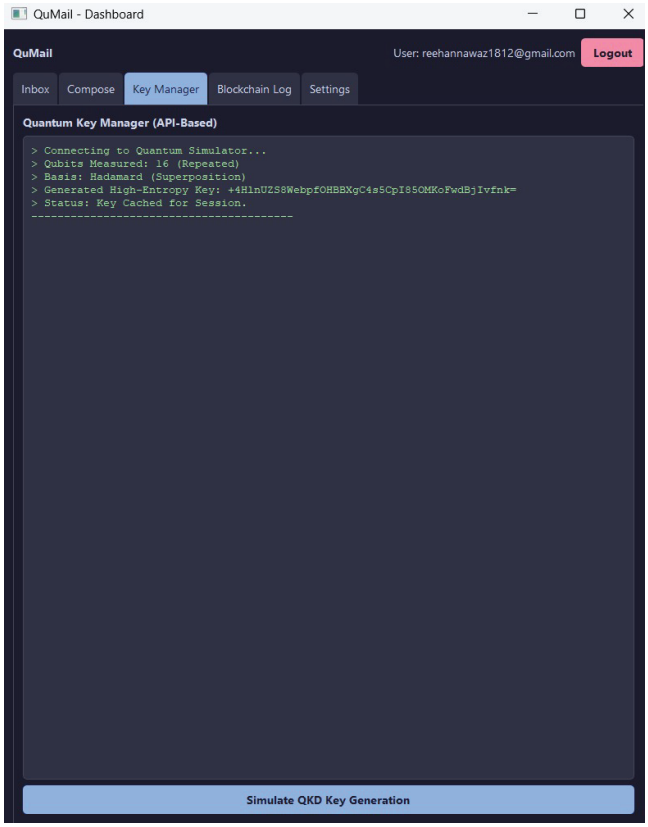

Fig. 5. QKD simulation log showing qubit preparation, basis selection, and key generation.

VI. Blockchain Audit Log

QuMail uses a light-weight blockchain module inspired by distributed ledger concepts [14] to log all cryptographic events like key generation, message encryption and decryption to ensure non-repudiation and tamper evident logging.

Each block in the ledger contains:

- Timestamp of the transaction
- Sender and receiver identifiers
- Applied security level
- SHA-256 hash of the encrypted payload
- Hash of the block behind it

The integrity for the blockchain ledger is used by a cryptographic hash chaining mechanism as

$$Hash_i = SHA256(Block_i || Hash_{i-1})$$

where $Hash_i$ represents the hash of the current block, $Block_i$ contains the transaction metadata, and $Hash_{i-1}$ represents the hash of the block behind the chain. This linking mechanism ensures that any modification to a previous block changes the hash values of next blocks, enabling immediate detection of tampering.

Any attempt to alter historical records generates a hash mismatch, which immediately reveals tampering within the blockchain ledger. The blockchain log is live and also can be refreshed from the user interface. This provides forensic traceability of communication events and verifiable proof of message transport and encryption, but without exposing plaintext.

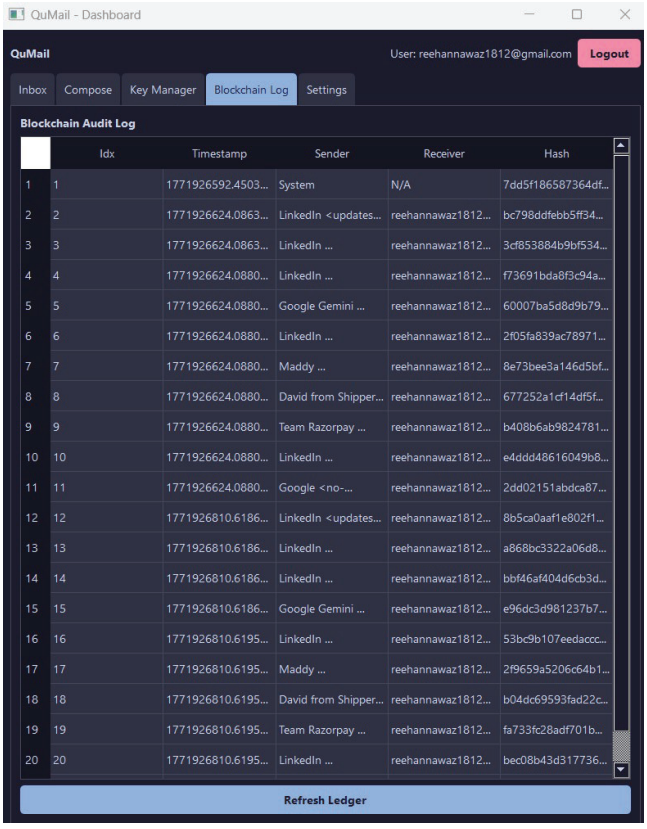

Fig. 6. Blockchain ledger providing tamper-evident audit trail of cryptographic operations.

VII. End-to-End Security Workflow

The operational workflow is as follows:

1) User authentication via secure login
2) QKD key generation and caching
3) Security level selection during message composition
4) Local encryption of message payload
5) Blockchain entry creation for the transaction
6) SMTP transmission of encrypted MIME payload
7) Receiver retrieves email via IMAP
8) Key retrieval and integrity verification
9) Decryption and plaintext rendering

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

VIII. Experimental Results

A QuMail prototype was tested in a production environment with a Gmail account to demonstrate interoperability with existing email infrastructure. We conducted experiments on functional correctness, encryption–decryption latency, key generation performance, and blockchain integrity.

A. Test Environment

We implemented the system in a Windows environment with an Intel processor and 8GB RAM. IBM Qiskit was used to run the simulation of QKD, and emails were sent using Gmail SMTP and IMAP servers through TLS.

B. Functional Validation

The following operational scenarios were tested:

- Successful user authentication and secure IMAP/SMTP session establishment
- Inbox synchronization and MIME parsing of encrypted payloads
- Multi-level encryption and decryption for Level 1 (RSA-AES), Level 2 (CRYSTALS-Kyber), and Level 3 (QKD-based OTP/AES)
- Single-use enforcement of QKD keys in OTP mode
- Real-time blockchain logging of cryptographic events

All test cases resulted in correct message recovery at the receiver without data loss.

C. Comparison with other Email Security

To find the efficiency of already proposed QuMail architecture, comparison was performed with commonly used secure email mechanisms. Traditional systems such as PGP and S/MIME rely on classical public-key cryptography, which can lead to quantum attacks. In contrast, the proposed QuMail system integrates post-quantum cryptography and QKD-based key generation to provide quantum-resilient security.

TABLE I
Comparison of Email Security Approaches

Method	Security Type	Latency
PGP	Classical	Low
S/MIME	Classical	Low
PQC (Kyber)	Quantum-resistant	Medium
Proposed QuMail	Hybrid QKD + PQC	Medium

D. Performance Analysis

The key generation, encryption, and decryption averages were recorded over several experiments. QKD key generation using Qiskit exhibited higher latency than classical key generation due to the computational overhead of quantum circuit simulation. However, encryption/decryption times after generation and caching were similar to those of classical AES operations.

The time for SMTP transmission was unaffected because the encryption happened on a local machine before the network transfer. To evaluate the computational overhead introduced by different security mechanisms, the average processing time for various cryptographic operations was measured.

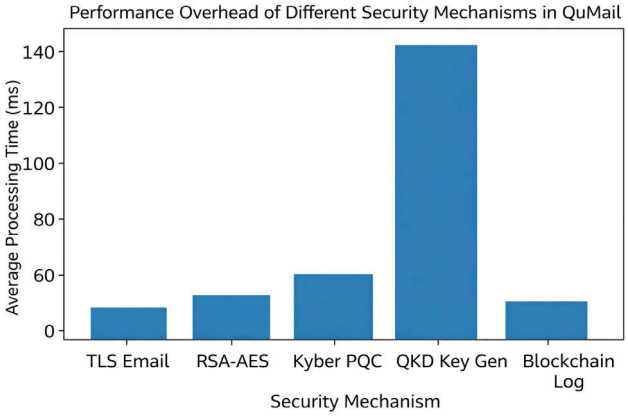

Fig. 7. Performance overhead comparison of different security mechanisms used in the QuMail system.

As illustrated in Fig. 7, QKD key generation introduces the highest computational overhead due to quantum circuit simulation performed by Qiskit. Classical TLS-based email communication exhibits the lowest latency because encryption occurs at the transport layer. The hybrid RSA-AES scheme introduces moderate overhead due to public-key operations during key exchange,while the CRYSTALS-Kyber post-quantum algorithm shows slightly higher computational cost due to lattice-based cryptographic computations. Despite these differences, the overall communication latency remains within acceptable limits for practical email communication systems.

E. Comparative Cryptographic Performance

To further find the efficiency of the system, a comparison was conducted between classical RSA-based encryption, post-quantum CRYSTALS-Kyber, and QKD-based key generation mechanisms.

The comparison focuses on key generation time, encryption latency, and computational complexity observed during the experiments.

TABLE II
Comparison of Cryptographic Mechanisms

Algorithm	Key	Security	Time (ms)
RSA-2048	Public Key	Classical	15–25
Kyber	PQC	Quantum-safe	20–30
QKD (BB84)	Quantum Key	Info-Theoretic	120–180

As shown in Table II, RSA provides lower computational latency due to its optimized classical cryptographic implementation. The CRYSTALS-Kyber algorithm introduces slightly higher computational cost because of lattice-based mathematical operations required for post-quantum security. In contrast, QKD-based key generation shows the highest latency due to quantum circuit simulation overhead in Qiskit. However, QKD provides information- theoretic security through one-time pad

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

TABLE III
AVERAGE CRYPTOGRAPHIC OPERATION TIME

Operation	Average Time (ms)
QKD Key Generation (Qiskit)	120–180
RSA-AES Encryption	15–25
Kyber Encryption	20–30
AES Decryption	10–15
Blockchain Block Creation	5–8

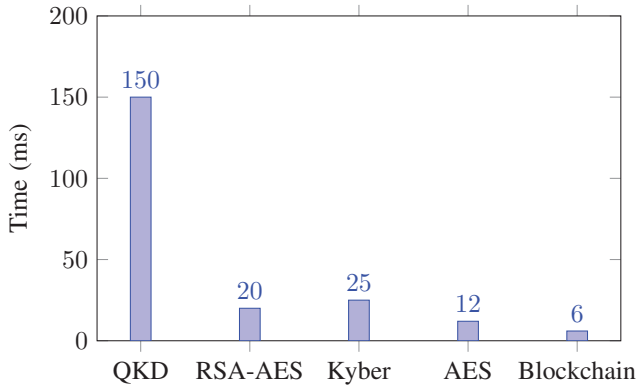

Fig. 8. Comparison of average latency for cryptographic operations used in the QuMail system.

encryption, which offers stronger long-term confidentiality compared to classical public-key methods.

F. Blockchain Integrity Verification

During each encryption and decryption operation, a block containing transaction metadata and hash pointers was added to the blockchain ledger. Multiple transactions were validated in order to ensure that hashes matched and the chain was valid. Modifying the static blocks manually led to a mismatch in hashes indicating effective tamper detection.

G. Interoperability

Using no server-side configuration, the prototype was able to send emails through Gmail encrypted. Encrypted messages were then sent as MIME attachments, ensuring compatibility with existing email protocols.

H. Discussion

These results demonstrate that quantum-resilient encryption mechanisms can be deployed at the application layer and integrated into existing email workflows without modifying underlying server infrastructure [8], [20]. QKD simulation incurs extra latency in key generations, but results in high-entropy keys that enable OTP based perfect secrecy. This blockchain module provides verifiable auditability without revealing any plaintext content.

These findings validate the feasibility of deploying hybrid quantum-safe email systems using existing infrastructure.

Fig. 8 illustrates the comparative latency of different cryptographic operations used in the QuMail system. QKD key generation exhibits the highest processing time due to quantum circuit simulation, whereas AES decryption and blockchain logging introduce minimal computational overhead.

IX. CONCLUSION

This paper presented QuMail, a quantum-resilient secure email framework that integrates Quantum Key Distribution (QKD) simulation, Post-Quantum Cryptography (PQC), and blockchain-based audit logging within a unified architecture. The proposed system shows that it's possible to use quantum-resistant security at the application level while still working smoothly with existing email systems that rely on SMTP and IMAP.

Experimental results show that the proposed approach provides strong cryptographic security with minimal communication overhead, while enabling tamper-evident logging of email transactions. Although QKD key generation introduces additional latency due to quantum circuit simulation, the overall impact on email delivery remains limited.

Future work will focus on integrating hardware-based QKD systems, optimizing key generation performance, and extending the architecture to support secure real-time communication applications such as encrypted messaging and video conferencing. These results demonstrate the practicality of deploying quantum-resilient communication systems on existing internet infrastructure without requiring fundamental changes to current email protocols.

ACKNOWLEDGMENT

Sincere gratitude to our institution and Computer Science and Engineering department for their support in conducting this research. We also express our sincere gratitude to our project guide who provided valuable technical guidance and constant encouragement in making QuMail a realisation.

Our sincere gratitude goes to: IBM Qiskit, used for simulating quantum key distribution; the ETSI GS QKD 014 specification which served as a reference for designing this key management interface. We also thank the developers of open-source cryptographic libraries and NIST Post-Quantum Cryptography standardization initiative for making CRYSTALS-Kyber algorithm specifications available to us, which are used in this work.

Last but not least, we thank the organizers behind the ISRO problem statement for pushing research in quantum-secure communication as well as providing a stage to build practical quantum-resilient applications.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, 1984.
[2] ETSI GS QKD 014, "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery APIs," ETSI, 2019.
[3] NIST, "CRYSTALS-Kyber Algorithm Specifications," 2023.
[4] IBM, "Qiskit: An open-source framework for quantum computing," 2024.
[5] W. Stallings, *Cryptography and Network Security*, Pearson, 2017.
[6] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*, 2020.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

[7] S. Pirandola et al., "Advances in Quantum Cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.
[8] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.
[9] NIST, "Post-Quantum Cryptography Standardization," National Institute of Standards and Technology, 2023.
[10] S. Garfinkel and S. L. Miller, "Johnny 2: A user test of key continuity management with S/MIME and Outlook Express," in *Proc. Symposium on Usable Privacy and Security (SOUPS)*, 2005.
[11] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.
[12] L. Chen et al., "Report on Post-Quantum Cryptography," NIST Interagency Report 8105, National Institute of Standards and Technology, 2016.
[13] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009.
[14] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[15] M. Peev et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, 2009.
[16] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, pp. 595–604, 2014.
[17] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, pp. 145–195, 2002.
[18] ETSI, "Quantum Key Distribution (QKD); Security Proofs and Protocol Implementation," ETSI GS QKD 001, 2019.
[19] V. Scarani et al., "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, 2009.
[20] H. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.
[21] S. Fluhrer, "Cryptanalysis of lattice-based cryptography," *IACR Cryptology ePrint Archive*, 2016.
[22] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2020.
[23] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[24] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
[25] T. Jager et al., "On the security of TLS 1.3 and QUIC against weak randomness," in *Proc. IEEE Symposium on Security and Privacy*, 2020.
[26] J. Ding and B.-Y. Yang, "Multivariate public key cryptography," in *Post-Quantum Cryptography*, Springer, 2009.
[27] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, pp. 351–382, 2016.
[28] M. Razavi, *An Introduction to Quantum Communications Networks*. Morgan & Claypool Publishers, 2018.