International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 06 June-2026 | Impact Factor: 3.5

Layered Post-Quantum Cryptography: A Dual-Encryption Approach to Mitigate Quantum Threats

Deepak Kushwah[1]*, Deepanshi Kushwah[1], Diwakar Shrivastava[2], Vijay Subhas Katta[2]

[1] Department of CSE, Hindustan College of Science and Technology, Mathura, India
[2] Assistant Professor, Department of CSE, Hindustan College of Science and Technology, Mathura, India

*Corresponding Author Email: deepak879142@gmail.com

How to Cite this Article:

Kushwah, D. & Kushwah, D. (2026). Layered Post-Quantum Cryptography: A Dual-Encryption Approach to Mitigate Quantum Threats. International Journal of Creative and Open Research in Engineering and Management, 02(6). https://doi.org/10.55041/ijcope.v2i6.338

https://doi.org/10.55041/ijcope.v2i6.338

Abstract—

The fast development of cyber communications, multimedia distribution, remote working have promoted the demand to transmit sensitive information through secure means in both the public and the private networks. The advent of massive quantum computers is rendering traditional cryptographic algorithms like RSA and Elliptic Curve Cryptography (ECC) insecure because they can crack the classical public-key algorithms like the Shor and Grover algorithms. This brings an immediate need of hybrid cryptographic systems, which integrate classical, quantum, and post-quantum algorithms to provide confidentiality, integrity, authentication, and future security beyond the quantum threat horizon.The paper is a proposal of a Hybrid Quantum-Post-Quantum Cryptographic Framework of transmitting files safely. It starts by aggregating files, which is a process to compress several files, images, videos, and multimedia files that users have chosen into one file to minimize redundancy and ease encryption. The AES-256 encrypted file is in GCM mode and provides confidentiality and integrity of the compressed file.The dual-layer mechanism ensures key establishment security. To begin with, Quantum Key Distribution (QKD) based on the protocols of BB84/E91 allows the Sender and the Receiver to generate a Quantum Secret Key (QSK) by exchanging quantum bits in quantum channel. Constant monitoring of the error rate facilitates automatic eavesdropping detection, and guarantees the keys generation is made when the conditions are secure, as well as the safeguarding of interception and man-in-the-middle attacks.A post-quantum layer is provided to ensure long-term security against quantum cryptanalysis, which uses Kyber, a NIST-approved lattice-based Key Encapsulation Mechanism (KEM). The Receiver creates a key pair of Kyber and disseminates the public key to the Sender. By using encapsulation, the Sender gets a PQC ciphertext and a Shared Secret (SS), with decapsulation on the Receiver side giving ensure that only participants of good faith get the same secret value.The hybridization phase consists of combining the QSK of QKD and SS of Kyber with the help of HKDF-SHA256 to obtain a Final Wrap Key (FWK). AES-GCM encrypts the key of file encryption by wrapping it with FWK which allows a secure and authenticated transfer of the key. The Sender sends four messages: encrypted file, Kyber ciphertext, wrapped AES key and the initialisation vector. At Receiver end, FWK is calculated once again with the help of QSK and SS so that the original data can be decrypted with the help of AES key.The suggested framework provides a defense-in-depth solution based on the combination of quantum security, post-quantum resilience and authenticated symmetric encryption. It can be analyzed that there is a strong resistance to classical and

quantum adversaries, scalability, and compatibility with the existing communication networks. This renders the model to be appropriate to secure government communication, military systems, data exchange in healthcare environments, cloud storage and financial infrastructures.

Keywords— Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), Kyber,Key Encapsulation Mechanism (KEM), HKDF-SHA256, Quantum Secret Key (QSK), GCM Mode.

I. INTRODUCTION

The issue of data security also plays a vital role in the contemporary computer-related activities and the emergence of quantum computing, which could endanger the current encryption techniques. The classical encryption algorithms such as AES and RSA can be susceptible to quantum attacks. Having that said, the combination of Quantum Cryptography, namely, Quantum Key Distribution (QKD) is a groundbreaking solution as it guarantees theoretically unbreakable encryption keys. The proposed system incorporates file compression, multi-layers encryption and multi-method key distribution. To begin with, the system can accept any file type, such as documents, pictures, videos, executables, and compress them into one ZIP file to save or send them in the most effective way possible. This is followed by classical encryption (AES/RSA) of the ZIP file that encrypts the data. The encryption keys are then encrypted using another layer of encryption with the principles of Quantum Cryptography to protect the keys in case of being intercepted. The reverse decryption is carried out based on the asymmetric cryptography principles, and only the recipients that are authorized can decrypt the files. Its high-tech multi-method key distribution is another added advantage that introduces redundancy and security through the distribution of keys in various secure channels and interception is virtually impossible. The project forks traditional encryption and prepares the data protection against the threat posed by quantum threats.

II. LITERATURE REVIEW

This focus on post-quantum cryptography (PQC) has been emphasized in recent years, as a means to protect future communication systems. Lohmiller et al. (2025) talked about the transition of vehicular networks to PQC and showed how hybrid certificates can be used to establish secure and efficient communications. The authors, however, noted that there are no practical implementations in real vehicular environments and migration strategies yet.

Study on Quantum era network security shows that combining Quantum Key Distribution (QKD) and PQC can enhance the security. Secure quantum communication was shown to be feasible in studies on Enhanced Network Security Protocols for the Quantum Era and Experimental Composable DM-CVQKD. However, such methods are costly to implement, have a short communication range and require further empirical testing.

In an extensive comparison of classical, quantum, and post-quantum cryptographic techniques, Sharath et al. (2025) reviewed the strengths and weaknesses of the methods.Sharath et al. (2025) compared classical, quantum, and post-quantum cryptographic techniques in great detail, explaining the advantages and disadvantages of the methods. Their contributions pointed out the weaknesses of traditional algorithms in the face of quantum attacks and the benefits of lattice-based PQC. But some practical deployment issues, hardware constraints, and the lack of global standards are important problems to address.

There are several researches on hybrid cryptographic systems based on classical cryptography, PQC and QKD. S. Ricci et al. (2024) presented a hybrid key management framework that showed better security and migration. Hybrid systems provide more resilience, but are also more complex and generally not standardized, restricting their use.

Studies related to critical infrastructures and privacy protection have also stressed the necessity of quantum-resistant security mechanisms. Current surveys show that PQC is a promising option for the security of intelligent and industrial infrastructures,

but most solutions are still in experimental stages and require comprehensive field tests. These constraints inspire the creation of a viable hybrid model that can offer both existing and emerging security solutions.

From the literature reviewed, it can be concluded that the current methods are either only PQC or QKD. There are few studies that combine both of the technologies into a common framework for secure multimedia file transmission. Hence, in this work, a Hybrid Quantum–Post-Quantum Cryptographic Framework is proposed, which incorporates AES-256, BB84 based QKD and CRYSTALS-Kyber to ensure improved security against classical and quantum adversaries. broader research context.

III. METHODOLOGY

The proposed Hybrid Quantum–Post-Quantum Cryptographic Framework aims to ensure the secure and future-proof transmission of multimedia and confidential files. The framework combines techniques such as file compression, symmetric encryption, Quantum Key Distribution (QKD), and Post-Quantum Cryptography (PQC) to create a multi-layer security structure.

Several files (such as documents, images, video, and other multimedia files) are first compressed into a single ZIP file, based on user selection. The compression removes redundancy, decreases storage space and makes data encryption easier because it is treated as a whole. In this way, the efficiency of transmission is increased and at the same time it provides compatibility with various file formats.

The compressed ZIP archive is then symmetrically encrypted with Advanced Encryption Standard (AES-256). For each session of transmission a random AES key and AES Initialization Vector (IV) are generated. The data in the ZIP file is encrypted with AES-256 in GCM mode, ensuring its integrity and confidentiality. The result of this stage will be a file that is encrypted and is called data.zip.enc.

The framework uses Quantum Key Distribution (QKD) on top of the BB84 protocol to provide secure key exchange. Quantum communication channel is set up between the sender and the receiver, by which the exchange of quantum bits takes place. A Quantum Secret Key (QSK) is generated after performing key sifting and error-rate analysis. The system is constantly checking the Quantum Bit Error Rate (QBER) to decide whether any eavesdropping has happened. The QSK is only accepted if the communication channel has been determined to be secure.

A post-quantum security layer is also put in place using the CRYSTALS-Kyber Key Encapsulation Mechanism (KEM). The receiver creates a Kyber public-private key pair and then sends the public key to the sender. The sender uses the public key of the receiver in order to find a shared secret (SS) and a resulting ciphertext.Based on the receiver's public key, the sender encapsulates to create the ciphertext and a shared secret (SS). Ciphertext is sent to the recipient and the shared secret is known only by the legitimate communicating parties.

The proposed framework also enhances security by using the Quantum Secret Key provided by QKD in addition to the shared secret provided by Kyber. The two secrets are used with the HKDF-SHA256 key derivation function to generate a Final Wrap Key (FWK). The FWK is then used to securely wrap the AES session key with AES-GCM, further enhancing the protection of the encryption key.

In secure transmission, the sender sends the encrypted ZIP archive, Kyber ciphertext, wrapped AES session key and Initialization Vector to the receiver. On the receiver side, the received QSK is obtained via the QKD process, and the Kyber private key decrypts the ciphertext and re-generates the shared secret. Subsequently, the receiver combines the QSK and shared secret to reproduce the Final Wrap Key. This key is used to decrypt the AES session key, which in turn, decrypts the encrypted archive and recovers the original multimedia files without any loss of information.

process involved a mixed-methods approach, combining quantitative surveys with qualitative interviews. A sample of 500 participants was recruited using stratified random sampling to ensure representation across demographic groups. Statistical analysis was conducted using SPSS software, while qualitative data was coded and analyzed thematically using NVivo.

IV. RESULTS AND DISCUSSION

Present your research findings clearly using tables, figures, and charts. Provide adequate

1.Sensitive Data Compression and Encryption

Feature:AES-256 Encryption Module and Secure File Compression.

A powerful algorithm that would be able to compress multiple file types in a single ZIP file and encrypt it using AES-256 to guarantee superb confidentiality.

2.Generation of Quantum-Secure Keys

Feature: Quantum Key Distribution (QKD)-Key Generation.

Implantation of Quantum Key Distribution (QKD) of generating the secret key that can never be intercepted or eavesdropped.

3.Post-Quantum Resilience

Feature: Lattice-Based Post-Quantum Cryptography with Kyber.

The use of lattice based cryptography (Kyber) to secure data against attacks in the future by the power of quantum computing which provides long encryption capacity.

4.Combination of Encryption Structure

Feature: Dual-layer Hybrid Encryption Architecture.

An encryption based on a dual-layered encryption with post quantum security and classical encryption of AES to implement multi-level encryption.

5.End-to-End Secure File Transfer

Feature: End-to-End Encryption of the Communication Pipeline.

A comprehensive transmission mechanism where encrypted data, keys and metadata can be transmitted safely and then correctly decrypted by the receiver with no data loss.

6.Detection of Errors and Data integrity

Feature: Mechanism of Checking Integrity and Eavesdropping.

53 Checking data integrity during encryption and decryption process and key generation and verification Eavesdropping attacks.

7.Scalability and Real-World Usability

Feature: Scalable and Multimedia-Compatible Architecture.

The architecture that has evolved to support a number of multimedia files and has the ability to handle bigger files without any hitch so as to be applicable to the actual secure communication needs. 7.8 Future-Proof Security Model Feature: Forward-Compatible Framework of Security Resistant to quantum attacks. A demonstration of a progressive compatible cybersecurity product that would not be broken in the classical and quantum computing periods.

Table I:Proposed System Results

Parameters	Data A	Data B
QBER	0%	0.001%
Encryption Time	10.013 sec	9.876 sec
Decryption Time	15.581 sec	15.826 sec
Key length	534 Bytes	498 Bytes
Hash difference	0%	0%

V. CONCLUSION

A project report on the creation of a combined cryptographic system called a hybrid cryptographic system was created to design and build a new hybrid cryptographic framework. The new system will utilize both classical (traditional) as well as post-quantum (21st-century) and quantum key distribution (QKD) to create a means for secure transmission of data for future quantum computing. The system uses a combination of many separate systems and methods of securing data (classical and post-quantum), making it the best available method to implement all possible available methods of securing data. The implementation of the new system begins with compressing the files, allowing the greatest level of possible efficiency in both storage and transmission. The next layer implements AES-256 encryption for data to create a secure and efficiently transmit. The third layer adds CRYSTALS-Kyber, a lattice-based post-quantum (lattice-based) algorithm, to protect

encrypted keys. Lastly, the final layer utilizes QKD (Quantum Key Distribution) as is based on the BB84 protocol, creating an arguably secure method of key generation; any attempt to eavesdrop on the key(s) will be detectable due to the laws of quantum mechanics(Fathalla & Azab, 2024). The project has integrated two different key derivation methods to provide an ultra-secure means of generating encryption keys, which are used to protect data as it is transmitted over an untrusted network. In this way, it also provides a better solution to the key interception problem than traditional key distribution methods. In addition, the Incremental System Development Life Cycle (SDLC) model used in the development and implementation of the project allows for a systematic and rigorous approach to developing, testing, and integrating all components of the system to reduce errors and ensure that the system functions as intended. As a result of this project, all file types can be managed securely 60 while maintaining data integrity, and the system provides complete end-to-end secure communication(Irshad et al., 2023). In summary, the system provides a secure and scalable solution for transmitting data with confidence in the future. The system is well positioned to handle current cyber threats and will be positioned to address potential quantum computing-related threats when they become foreseen, making this project an excellent candidate for next-generation cybersecurity solutions.

REFERENCES

[1] Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F.D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P. and Hansen, R., 2022. Transitioning organizations to post-quantum cryptography. Nature, 605(7909), pp.237-243.

[2] Dam, D.T., Tran, T.H., Hoang, V.P., Pham, C.K. and Hoang, T.T., 2023. A survey of post-quantum cryptography: Start of a new race. Cryptography, 7(3), p.40.

[3] Cherkaoui Dekkaki, K., Tasic, I. and Cano, M.D., 2024. Exploring post-quantum wcryptography: Review and directions for the transition process. Technologies, 12(12), p.241.

[4] WinZip Documentation, 2020, Mosca, 2018, NIST, 2022, Bennett and Brassard, 1984, ISRO, 2021.

[5] Fernandez-Carames & Fraga-Lamas, 2020, Ralegankar et al.2022, Ricci et a., 2024, Khan et al., 2024, Irshad et al., 2023, Rubio García et al., 2025

[6] Lohmiller, J., et al., 2025. A survey of post-quantum cryptography migration in vehicles.

[7] Rubio García, A., et al., 2025. Enhanced network security protocols for the quantum era.

[8] Hajomer, A., et al., 2025. Experimental composable key distribution using discrete-modulated continuous variable quantum cryptography.

[9] Sharath, M., et al., 2025. Quantum-resilient cryptography: A survey on classical & quantum algorithms.

[10] Oliva Del Moral, P., et al., 2024. Cybersecurity in critical infrastructures: A post-quantum cryptography perspective.

[11] Ricci, S., et al., 2024. Hybrid keys in practice: Combining classical, quantum & post-quantum cryptography.

[12] Näther, S., et al., 2024. Migrating software systems toward post-quantum cryptography — A systematic literature review.

[13] K. F. Hasan et al., "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies," IEEE Access, vol. 12, pp. 23427–23450, 2024.

[14] K. K. Singamaneni et al., "A Novel Hybrid Quantum-Crypto Standard to Enhance Security and Resilience in 6G-Enabled IoT Networks," IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens., vol. 18, 2025.

[15] P. Radanliev, "Artificial Intelligence and Quantum Cryptography," Journal of Analytical Science and Technology, vol. 15, no. 4, 2024.

[16] E. Fathalla and M. Azab, "Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security,

and Optimizations," IEEE Access, vol. 12, pp. 175969–175987, 2024.

[17] Y. Karli et al., "Controlling the Photon Number Coherence of Solid-State Quantum Light Sources for Quantum Cryptography," npj Quantum Information, vol. 10, no. 17, 2024.

[18] M. A. Khan et al., "Future-Proofing Security for UAVs With Post-Quantum Cryptography: A Review," IEEE Open Journal of the Communications Society, vol. 5, pp. 6849–6870, 2024.

[19] P. K. Maduni et al., "Hybrid Quantum-Safe Cryptographic Scheme With Secure Key Exchange and Signature Scheme," IEEE Access, vol. 13, 2025.

[20] A. Castiglione et al., "Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices," IEEE Trans. Industrial Informatics, vol. 21, no. 2, pp. 1674–1683, 2025.

[21] R. R. Irshad et al., "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," IEEE Access, vol. 11, pp. 105479–105498, 2023.

[22] D. Shahwar et al., "Quantum Cryptography for Future Networks Security: A Systematic Review," IEEE Access, vol. 12, pp. 180048–180079, 2024.

[23] V. K. Ralegankar et al., "Quantum Cryptography-as-a-Service for Secure UAV Communication: Applications, Challenges, and Case Study," IEEE Access, vol. 10, pp. 1475–1490, 2022.

[24] D. S. C. Putranto et al., "Space and Time-Efficient Quantum Multiplier in Post Quantum Cryptography Era," IEEE Access, vol. 11, pp. 21848–21862, 2023.

[25] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," IEEE Access, vol. 8, pp. 21091–21116, 2020.

[26] P. W. Shor, ''Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,'' SIAM Rev., vol. 41, no. 2, pp. 303–332, Jan. 1999.

[27] D.Joseph, R.Misoczki, M.Manzano, J.Tricot, F.D.Pinuaga, O.Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, ''Transitioning organizations to post-quantum cryptography,'' Nature, vol. 605, no. 7909, pp. 237–243, May 2022.

[28] AUTOSAR. (2022). Specification of Secure Hardware Extensions. Accessed: Dec. 6, 2024. [Online]. Available: https://www.autosar.org/fileadmin/standards/R22-11/FO/AUTOSAR_TR_SecureHardware Extensions.pdf

[29] L.K.Grover, ''A fast quantum mechanical algorithm for database search,'' in Proc. 28th Annu. ACM Symp. Theory Comput., 1996, pp. 212–219.

[30] K. Schmeh, Kryptografie: Verfahren, Protokolle, Infrastrukturen. Heidel berg, Germany: Dpunkt.Verlag GmbH, 2016.

[31]Cooperative Intelligent Transportation Systems—Dedicated Short Range Communications—Part1:GeneralTechnicalRequirement,StandardGB/T 31024.1-2014, GB/T, 2014.

[32] M. Ziehensack and R. Pallierer. (2022). Secure Automotive Ethernet for Automated Driving—Multi-Level Security Architecture. Accessed: Dec. 6, 2024. [Online]. Available: https://www.elektrobit.com/blog/ automotive-ethernet-automated-driving-multi-level-security/

[33] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, ''Evaluation of CAN bus security challenges,'' Sensors, vol. 20, no. 8, p. 2364, Apr. 2020.

[34] A. Buntsma, S. Wilczek, C. de Laat, and C. Schappin. (2020). Cybersecurity in Automotive Networks. Univ. Project Rep. Accessed: Dec. 6, 2024.

[35] A. Happel. (2014). Secure Communication for CAN FD. CAN Newslett. Accessed: Dec. 6, 2024. [Online]. Available: https://cdn.vector.com/cms/

content/know-how/_technical-articles/Security_CAN_Newsletter_201411_PressArticle_EN.pdf

[36] B. Vinodh Kumar and J. Ramesh, ‘‘Automotive in vehicle network protocols,’’ in Proc. Int. Conf. Comput. Commun. Informat., Jan. 2014, pp. 1–5. [37] IEEE Standard for Ethernet Amendment 1: Physical Layer Specifications and Management Parameters for 100 Mb/s Operation Over a Single Balanced Twisted Pair Cable (100BASE-T1), IEEE Standard 802.3bw 2015, 2016.

[37] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, ‘‘CRYSTALS-dilithium: A lattice-based digital signature scheme,’’ IACR Trans. Cryptograph. Hardw. Embedded Syst., vol. 2018, pp. 238–268, Feb. 2018.

[38] B. Westerbaan. (2022). NIST’s Pleasant Post-Quantum Surprise. Accessed: Dec. 6, 2024. [Online]. Available: https://blog.cloudflare.com/nist-post-quantum-surprise/

[39] J. V. Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, and A. Cleven, ‘‘Reconstructing the giant: On the importance of rigour in documenting the literature search process,’’ in Proc. Eur. Conf. Inf. Syst., 2009, pp. 1–14.

[40] N. Alnahawi, A. Wiesmaier, T. Grasmeyer, J. Geißler, A. Zeier, P. Bauspieß, and A. Heinemann, ‘‘On the state of post-quantum cryptogra phy migration,’’ in Proc. INFORMATIK, 2021, pp. 907–941.

[41] Khan, U.H., Qamar, A., Khan, R., Alawad, M.A., Alturise, F. and Hayat, M., 2025. TrustEdge: A Quantum-Safe, Self-Healing Framework for Federated TinyML in Critical ICU Monitoring. Internet of Things, p.101855