WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Comparative Study of Hybrid Cryptographic Systems: Integrating Classical and Post-Quantum Cryptographic Techniques for Comprehensive Post-Quantum Security

Thafzy V M[1], Dr. Nikesh P[2]

[1]Department of Computer Science and Engineering Government Engineering College, Wayanad (AICTE,KTU), Kerala, India thafzyvm@gmail.com
[2]Department of Computer Science and Engineering Government Engineering College, Wayanad (AICTE,KTU), Kerala, India nikeshp@gecwyd.ac.in

ABSTRACT—

The rise of quantum computer made a significant threat to traditional cryptographic protocols which figured out the importance of implementing hybrid approaches which integrate classical and post quantum cryptographic techniques. In this overview, we analyze different areas where quantum computing technique is implemented and how it has contributed to those applications. Traditional encryption schemes like RSA and ECC can be attacked by quantum algorithm which necessitating the need for quantum resistant technique. The research includes the evaluation of different systems where the classical system are integrated with post quantum cryptographic algorithm. Besides, discuss and analyze the seamless working of existing network layer protocols with quantum algorithms. This survey provides a foundation for protecting systems from upcoming quantum threats, which describes the advancements in post-quantum algorithms and quantum cryptography.

***Index Terms*—Hybrid cryptography, post-quantum cryptography, key exchange mechanisms, cryptographic security, IND- CCA, ECDH.**

I. INTRODUCTION

The growing development of quantum computing pose serious challenges to traditional cryptography systems. One of the main risks created by quantum computing is its potential to overcome classical public key encryption by utilizing techniques like Shor's algorithm. These consist of the Elliptic Curve Discrete Logarithm Problem (EC-DLP), the Discrete Logarithm Problem (DLP), and the Integer Factorization (IF) problem. Classical cryptographic techniques like RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) are based on these issues. These cryptographic protocols may be broken by quantum computers once they are powerful enough, making them useless and jeopardizing the security of contemporary communication systems. This emerging risk has highlighted the urgent need to develop cryptographic solutions that can resist quantum attacks.

Hybrid cryptography systems have become a viable solution to these issues and a promising way to protect sensitive communications. These systems integrate cryptographic primitives from several paradigms: classical, post-quantum, and quantum cryptography.

The hybrid technique capitalizes on the time-tested dependability of classical cryptographic algorithms, combines the quantum resistance of post-quantum cryptography (PQC), and uses the potentially unbreakable security afforded by quantum key distribution (QKD). By integrating these strategies, hybrid cryptographic systems strive to guarantee robust protection against both classical and quantum adversaries. Importantly, such systems also permit a smooth transition to the post-quantum era, bridging the gap between contemporary cryptographic methods and the future need for quantum-safe solutions.

The significance of hybrid cryptography is emphasized by a number of international standards and recommendations. For example, the Federal Office for Information Security (BSI) and the European Network and Information Security Agency (ENISA) recommend combining pre-quantum and post-quantum cryptographic algorithms to reduce risks, highlighting the need for cryptographic schemes that can be implemented in existing infrastructures without creating vulnerabilities like downgrade attacks, and hybrid systems are crucial for resolving the uncertainties surrounding post quantum cryptographic algorithms, which have not been as thoroughly tested or as extensively used as classical methods. In order to overcome these difficulties, a unique hybrid cryptographic system is presented in this research. The system has been shown to be safe from chosen cipher text assaults (IND-CCA) and secure in the quantum standard model. Additionally, it is made to be resource-efficient, versatile enough to work with or without the quantum component, and able to run on small FPGA platforms. Because of these characteristics, it may be easily integrated with other cryptographic protocols, including TLS 1.3, allowing for real-world implementation in high security settings.

This hybrid system provides a strong and scalable way to protect sensitive data in the quantum era by utilizing the combined advantages of classical, post-quantum, and quantum cryptography techniques. It's potential for protecting vital applications, including as financial services, government communications, and vital infrastructure systems, is highlighted by its efficiency, agility, and compatibility with existing infrastructure.

II. LITERATURE REVIEW

A revolutionary era is being ushered in by quantum computing, which calls for a reassessment of traditional cryptography methods and motivates intensive research for quantum-resistant substitutes. The literature review that follows compiles findings from well-known research on the problems and solutions of quantum and post-quantum cryptography.

In a variety of application domains, Nagpal et al. [1] investigate how quantum computing can be incorporated into real-time cryptography systems. Their research highlights the pressing need for quantum-resistant cryptographic techniques by focusing on how quantum algorithms, like Shor's and Grover's, affect conventional cryptographic protocols. To protect data against quantum threats, new developments in hybrid cryptography—a combination of classical, post-quantum, and quantum techniques—are investigated. The authors also examine the practical difficulties of implementing quantum key distribution (QKD) in current communication systems and assess its suitability for use in vital industries like national security, healthcare, and finance. The groundwork for creating quantum-safe cryptographic solutions is laid by this thorough analysis.

Quantum Secure Direct Communication (QSDC), a revolutionary method that uses quantum mechanics to assure provably secure message transmission via quantum channels, is introduced by DongPan et al. [2]. QSDC provides secure message transmission that is impervious to quantum computing power, in contrast to QKD, which only concentrates on key creation. Eavesdropping can be detected thanks to theoretical developments in QSDC that take advantage of quantum entanglement and superposition concepts. Notwithstanding current obstacles like network scale and error correction, recent experimental confirmations highlight the viability of QSDC protocols. These results establish QSDC as a game-changing component of post-quantum secure communication systems.

A methodical methodology is put forth by Hasan et al.

[3] to help businesses make the switch to post-quantum cryptography. It is stressed how urgent it is to switch to quantum-resistant techniques since conventional systems like RSA and ECC are made vulnerable by quantum algorithms like Shor's. Using graph-theoretic methods to detect and rank cryptographic assets, their research outlines strategies for moving toward quantum-safe systems. The method offers a blueprint for future-proofing vital data against quantum threats while facilitating efficient resource allocation and integration with current organizational systems.

Quantum Key Distribution (QKD) is investigated by Biswas et al. [4] as a workable and viable defense against the dangers of quantum computing. Their study introduces advances such as a modified key-sifting scheme and Tree Parity Machine based analysis for key reconciliation, while highlighting the multi-stage processes required in QKD: raw key generation, key sifting, reconciliation, and privacy amplification. These improvements boost QKD's effectiveness and establish it as a key component of post-quantum secure communication.

In the fields of data science and web security, Shim et al.

[9] investigate sophisticated cryptographic methods designed to meet the twin difficulties of quantum and conventional threats. In order to create hybrid models that combine the scalability and efficiency of PQC techniques with the provable security of quantum mechanics, the study explores the integration of Quantum Key Distribution (QKD) with post-quantum cryptography (PQC) approaches. The optimization of these protocols for vital online security applications such as safe data transfer, authentication systems, and defense against quantum-powered attacks is the main focus. Along with examining cutting-edge machine learning-driven data security applications, the authors offer frameworks for fortifying the cryptographic backbone of contemporary web systems. Through theoretical analysis and practical insights, the study addresses key challenges, such as latency, computational overhead, and adaptability, marking a significant step towards robust quantum-secure frameworks for the digital era.

The article by Christian Nather et al. [6] addresses the vulnerabilities posed by quantum computing and offers a thorough architecture to make the transition of software systems to post-quantum cryptography (PQC) easier. In order to identify crucial cryptographic assets and dependencies in current systems, their method places a high priority on a structured security dependency analysis. The study presents graph theoretic approaches for assessing these relationships, enabling enterprises to gradually switch to quantum-resistant algorithms like hash or lattice-based schemes. The authors illustrate real world application scenarios through thorough case studies, showing how businesses can incorporate PQC techniques without seriously interfering with ongoing operations. This study offers a path for enterprises to safeguard their software systems in anticipation of the upcoming post-quantum age by striking a balance between operational continuity and future proofing against quantum risks.

A complete quantum key management system (KMS) is designed by Shim et al. [10] to address weaknesses revealed by quantum algorithms such as Shor's. Through innovations like key relay and peer-to-peer techniques, the system incorporates symmetric key lifecycle management, enabling secure many-to-many communication. The suggested design shows great promise for practical implementation in networks such as Korea's KREONET, as confirmed by simulations.

In order to avoid the necessity for separate dark fibers, Sharma et al. [8] investigate the integration of QKD within optical networks. This paper offers a thorough analysis of QKD techniques and their uses, addressing issues with routing, wavelength allocation, resilience, and quantum key recycling. The optimization of the popular BB84 protocol for secure key formation over optical fiber networks and the prevention of quantum hacking assaults are given particular attention.

Khan and colleagues [7] examine how quantum attacks affect UAV security. The evaluation emphasizes the need to use PQC algorithms due to risks caused by open wireless channels and computational resource constraints. This work offers a strong basis for improving UAV resistance against changing quantum threats by analyzing NIST's PQC standardization progress and defining future research options.

In order to address the issue of increasing signature sizes, Kwon et al. [5] concentrate on hybrid cryptographic methods that combine classical and post-quantum signatures. By combining ECDSA P-256 with Falcon-512, their suggested approach produces small, safe signatures with little computational overhead. This small hybrid technique improves compatibility and creates a path for the smooth integration of classical and quantum-resistant cryptographic solutions, as demonstrated by experimental results on various platforms.

This survey provides a thorough overview of approaches and solutions addressing security concerns posed by quantum computing by synthesizing ground-breaking research in quantum and post-quantum cryptography. Every contribution highlights the team's combined efforts to create reliable quantum-secure systems for a range of application areas.

Elliptic Curve Diffie-Hellman (ECDH) and Post-Quantum Cryptography (PQC) combine to form a hybrid cryptography system that combines the advantages of quantum-resistant and conventional methods. Due to its effectiveness and widespread use, ECDH permits safe key transfers while guaranteeing compatibility with current systems. As a defense against quantum computer attacks, PQC enhances ECDH by mitigating its susceptibility to such dangers. This integration offers long term resilience in a changing threat scenario in addition to immediate security gains. Organizations can create a transitional framework by integrating these strategies, keeping up present operations while getting ready for quantum readiness. ECDH and a PQC method, like a key encapsulation mechanism (KEM) like Kyber or NTRU, are executed in parallel by the integration in practice. A final hybrid key is produced by combining the shared secrets produced by each algorithm using cryptographic methods like hashing. By using two keys, the system's security is not dependent on just one algorithm. The PQC component will continue to safeguard the key even if ECDH is compromised by a future quantum computer. On the other hand, ECDH's efficiency and resilience minimize performance overhead during the integration stage and offer an additional degree of security throughout the switch to quantum-resistant algorithms.

This hybrid strategy is especially useful in settings where proactive defenses are crucial but the hazards posed by quantum computing are not yet completely understood. Applications where maintaining long-term anonymity is crucial include financial transactions, secure communications, and the defense of vital infrastructure. By combining ECDH with PQC, systems are protected from known and unknown threats, offering future-proofing and cryptographic agility. This system can provide a seamless transition as cryptographic standards change to incorporate PQC, striking a balance between efficiency, backward compatibility, and quantum resistance. A strong security model that can handle the ever-changing problems of a post-quantum world is the end result.

III. METHODOLOGY

The approaches put forth in these papers show how cryptographic systems have evolved to incorporate quantum-safe solutions, progressively moving from classical cryptography to the use of quantum key distribution (QKD) and post-quantum cryptography (PQC) techniques. First, communication systems frequently employ traditional cryptographic methods for key exchange and encryption. Although these systems are susceptible to quantum attacks, they are currently regarded as secure. The articles outline the maintenance of classical protocols for key exchanges and real-time communications, using an established secure baseline [1]. A trend toward incorporating quantum-resistant approaches, including PQC algorithms, which offer resilience against quantum decryption techniques, is underway as quantum computer breakthroughs raise the possibility of cracking classical cryptography. As we get ready for the quantum era, this shift guarantees that these cryptographic systems stay safe, enabling businesses to protect their systems without interfering with ongoing operations.

Quantum key distribution (QKD) is a crucial mechanism to increase security in the quantum era. QKD distributes cryptographic keys securely over potentially insecure channels by utilizing quantum physics. To make sure that private key exchanges are safe from quantum eavesdropping, the techniques use QKD protocols like BB84, E91, and entanglement- based techniques. Advanced approaches like dense wavelength division multiplexing (DWDM) and the usage of quantum repeaters are proposed to overcome obstacles like signal loss and distance restrictions in optical fiber networks in order to increase the performance and scalability of QKD [2]. Furthermore, enhancing the QKD process—particularly by integrating it with artificial neural networks (ANNs)—introduces sophisticated machine learning methods to improve key reconciliation's dependability and efficiency. ANNs improve the overall robustness of the key distribution process by dynamically adjusting settings to correct discrepancies that occur during transmission [4].

Furthermore, the integration of PQC and quantum cryptography solutions shifts towards more sophisticated methods as enterprises seek to future-proof their systems. For instance, hybrid signature schemes that combine post-quantum and classical cryptography techniques are now under development. These hybrid techniques allow a smooth transition between compatibility with current systems and long-term resilience to quantum computing by combining conventional cryptographic signatures with quantum-resistant alternatives [5]. For resource-constrained situations, the paper's approaches minimize computational overhead by proposing a compact, effective hybrid signature strategy. Simultaneously, these investigations investigate organized systems that guarantee a seamless transition from traditional cryptography standards to quantum-safe substitutes. These frameworks prioritize the integration of quantum-resistant algorithms, like lattice-based and code-based encryption

and detect weak points in the cryptographic infrastructure by performing security dependence analyses. Case studies and real-world examples show how this planned migration may be accomplished in a variety of sectors, guaranteeing that systems stay safe during the smooth transition to PQC [3], [6].

Furthermore, quantum-safe cryptographic systems must be integrated into particular domains like unmanned aerial vehicles (UAVs), high-performance research networks like KREONET, and other security-sensitive applications. For example, using quantum-resistant algorithms designed for UAVs' constrained computational capabilities in place of traditional cryptographic techniques like RSA improves UAV security. These systems may function in a variety of settings thanks to a hybrid cryptography technique, which also makes them resistant to both conventional and quantum attacks. [7]. Similar to this, efficiently handling QKD key exchanges is a major component of the design of quantum key management systems for high performance networks like KREONET. These systems are scalable to meet the demands of a fast changing quantum world while addressing important issues like key lifetime, refreshment, and compatibility with current security protocols [10]. All things considered, the suggested approaches provide thorough frameworks for protecting communications from both classical and quantum threats as well as easing the shift to quantum-resilient systems for both new and pre-existing infrastructures.

When combined, these developing approaches seek to offer a comprehensive roadmap for protecting systems against quantum attacks, emphasizing the smooth integration and transition to quantum cryptography while maintaining performance, backward compatibility and future preparedness. To protect the world's communication infrastructure from future threats, it will be essential to integrate post-quantum algorithms, quantum cryptography protocols, and quantum key management.

IV. CHALLENGES AND FUTURE TRENDS

Traditional cryptography methods like RSA, ECC, and other algorithms that rely on the difficulty of factorization and discrete logarithms face serious issues as a result of the development of quantum computing. These cryptosystems can be successfully broken by quantum algorithms, such as Shor's and Grover's, making them outdated. Organizations must assess and improve their current infrastructure as part of the complicated and resource-intensive shift to quantum-resilient systems. Since post-quantum cryptography (PQC) techniques frequently bring bigger key sizes and more computational overhead, which can affect performance and scalability, interoperability and backward compatibility are also significant problems. Furthermore, a lot of testing and adaptation are needed to ensure the smooth integration of PQC with legacy systems, especially for businesses that depend on low-latency and resource-constrained devices like IoT and UAVs.

Finding a balance between security and performance is another significant difficulty. Although QKD is theoretically impenetrable, it has real-world problems such signal attenuation, short transmission ranges, and the requirement for quantum repeaters in big networks. Significant expense and complexity are added by the physical layer requirements, which include the usage of satellite links or optical fibers. Furthermore, post-quantum algorithms frequently need for more processing power and memory, which puts a burden on networks and devices already in place. Innovations in quantum-resistant algorithm designs that put efficiency, scalability, and compatibility first are needed to address these problems and make sure that these systems can fulfill real- world objectives without sacrificing security or usability.

The creation of hybrid cryptographic systems, which blend PQC and QKD with classical encryption, is one of the major new ideas. By enabling systems to function safely in mixed contexts where conventional and quantum risks coexist, hybrid techniques guarantee a seamless transition. Compact hybrid signatures are one example of a signature scheme advancement that aims to lower computational cost while preserving strong security features. Furthermore, research is increasingly focusing on optimizing QKD procedures through the integration of machine learning techniques such as artificial neural networks (ANNs). By increasing the precision of key reconciliation and error correction, these methods raise the general effectiveness and dependability of quantum-based systems.

Initiatives like NIST's post-quantum cryptography standardization process are fueling the global movement toward the adoption of standardized quantum-safe cryptographic systems. In parallel, these technologies are being tested and validated in operational settings for domain-specific applications including high-performance research networks and secure UAV communications. Large-scale quantum-safe communication infrastructure is feasible, as evidenced by the implementation of quantum key management systems (KMS) in networks like KREONET. The emphasis is now on creating robust, future-proof security architectures while researchers continue to tackle scalability and integration issues. By protecting vital data and systems against previously unheard-of computational power, this progression guarantees that enterprises stay flexible and ready for the impending quantum age.

V. CONCLUSION

With the revolutionary impact of quantum computing, key areas of progress are quantum and post-quantum cryptography. A proactive shift to quantum-resistant alternatives is required due to the imminent threat of quantum algorithms breaking traditional cryptography systems. This survey compiles a wealth of research investigating approaches that tackle the long-term need for future-proofing against quantum threats as well as the present need for secure communication. These solutions, which range from post-quantum cryptography (PQC) algorithms to quantum key distribution (QKD), open the door for strong cryptographic systems that can protect sensitive information and vital infrastructure.

The development of cryptographic approaches shows a distinct shift toward hybrid solutions, which combine quantum,

TABLE I

Comparative Analysis

Sl Not	***Title***	***Feature***	***Merits***	***Demerits***
1	Quantum Computing Integrated Patterns for Real-Time Cryptog-raphy in Assorted Domains	Combines quantum computing, classical cryptog-raphy, and post-quantum cryptography to enhance security across various domains.	Ensures future-proof, scalable, and efficient cryptographic solutions with real-time processing capabilities.	Faces im-plementation challenges and resource demands while relying on the adoption of emerging cryptographic standards.
2	The Evolution of Quantum Secure Direct Com-munication : On the Road to the Qinternet	Leverages quantum secure direct communica-tion (QSDC) and quantum networking to enable ultra-secure, direct message transmission without intermediate encryption.	Provides inherent eavesdropping detection and scalability for secure communica-tions over long distances using quantum repeaters.	Faces challenges in infrastructure development, cost, and efficient integration into existing communica-tion systems.
3	A Framework for Migrating to Post-Quantum	Proposes a structured migration framework using security	Ensures a seamless and prioritized migration while balancing	Migration complexity may vary across industries, requiring

	Cryptog-raphy: Security Dependency Analysis and Case Studies	dependency analysis and case studies to transition to post-quantum cryptography (PQC).	current security needs and future-proofing strategies.	extensive resources and customization for effective implementa-tion.
4	A Modified Key Sifting Scheme With Artificial Neural Network Based Key Reconcilia-tion Analysis in Quantum Cryptogra-phy	Enhances quantum key distribution with a modified key sifting scheme and artificial neural networks for efficient key reconcilia-tion.	Improves accuracy, error correction, and adaptability in key reconciliation while boosting overall system reliability.	Increases computational complexity and may require significant optimization for resource-constrained systems.
5	Compact Hybrid Signature for Secure Transition to Post-Quantum Era	Combines classical and post-quantum signature algorithms into a compact hybrid signature scheme for enhanced security.	Ensures backward compatibility, quantum resistance, and suitability for resource-constrained environments.	May involve added complexity in managing dual cryptographic components during the transition phase.

Sl No	***Title***	***Feature***	***Limitation***	***Merits***
6	Migrating	Provides a	Maintains	Requires

	Software Systems Toward Post-Quantum Cryptogra-phy	structured approach to transition software systems to post-quantum cryptography by identifying and replacing vulnerable components.	operational efficiency while ensuring security against quantum threats with minimal disruption.	significant effort in assessment, testing, and optimization for seamless integration of PQC algorithms.
7	Future-Proofing Security for UAVs With Post-Quantum Cryptogra-phy	Integrates post-quantum crypto-graphic algorithms into UAV communica-tion and data protection layers for enhanced security.	Ensures long-term resilience against quantum attacks while addressing real-time processing and resource constraints.	Involves high complexity in replacing existing protocols and balancing lightweight cryptographic needs.
8	Quantum Key Distribution Secured Optical Networks: A Survey	Explores integrating quantum key distribution (QKD) with optical networks using advanced protocols and optical	Enables secure, scalable, and eavesdropping-resistant key exchange over long-distance optical channels.	Faces technical challenges in implementa-tion, cost, and compatibility with existing optical network infrastructures.

		techniques like DWDM and quantum repeaters.		
9	Research on Quantum Key, Distribution Key and Post-quantum Cryptog-raphy Key Applied Protocols for Data Science and Web Security	Proposes a hybrid model integrating quantum key distribution and post-quantum cryptography for secure data science and web security protocols.	Ensures resilience against classical and quantum attacks while maintaining scalability and efficiency in real-time data operations.	Challenges include high computational demands and complexity in integrating advanced cryptographic techniques into existing frameworks.
10	Design and Validation of Quantum Key Management System for Construction of KREONET Quantum Cryptogra-phy Com-munication	Develops a quantum key management system for KREONET, enabling secure key generation, distribution, and storage for quantum cryptography communica- tion.	Enhances commu-nication security with robust key management and scalability tailored for high-performance networks.	Requires extensive validation and adaptation to ensure compatibility with existing infrastructures and manage implementa-tion costs.

PQC, and conventional methods to guarantee compatibility and robustness. The quick developments in improving scalability, performance, and security are demonstrated by innovations in machine learning integration, compact signatures, and effective key reconciliation techniques. Moreover, domain-specific applications in fields like as optical networks, high performance communication systems, and unmanned aerial vehicles (UAVs) show how versatile quantum-safe technologies are in a variety of industries. Even though there has been a lot of development, overcoming obstacles including high computing costs, interoperability, and deployment complexity is still necessary to achieve broad adoption.

Going forward, the shift to quantum-safe ecosystems will be greatly aided by international cooperation and standardization initiatives. Comprehensive security architectures are based on frameworks for structured migration, experimental validation of hybrid systems, and quantum technology breakthroughs. Industries can create robust infrastructures that can survive future quantum computing capabilities while maintaining data availability, security, and integrity in a quickly changing digital ecosystem by adopting these cutting-edge approaches.

References

[1] Nagpal, Shally, Shivani Gaba, Ishan Budhiraja, Meenakshi Sharma, Akansha Singh, Krishna Kant Singh, S. S. Aksar, Mohamed Abouhawwash, and Celestine Iwendi. ”Quantum Computing Integrated Patterns for Real-Time Cryptography in Assorted Domains.” IEEE Access (2024).

[2] Pan, Dong, Gui-Lu Long, Liuguo Yin, Yu-Bo Sheng, Dong Ruan, Soon Xin Ng, Jianhua Lu, and Lajos Hanzo. ”The evolution of quantum secure direct communication: on the road to the qinternet.” IEEE Communications Surveys and Tutorials (2024).

[3] Hasan, Khondokar Fida, Leonie Simpson, Mir Ali Rezazadeh Baee, Chadni Islam, Ziaur Rahman, Warren Armstrong, Praveen Gauravaram, and Matthew McKague. ”A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies.” IEEE Access (2024).

[4] Biswas, Chitra, Md Mokammel Haque, and Udayan Das Gupta. ”A modified key sifting scheme with artificial neural network based key reconciliation analysis in quantum cryptography.” IEEE Access 10 (2022): 72743-72757.

[5] Kwon, Hee-Yong, Indra Bajuna, and Mun-Kyu Lee. ”Compact Hybrid Signature for Secure Transition to Post-Quantum Era.” IEEE Access (2024).

[6] Na¨ther, Christian, Daniel Herzinger, Stefan-Lukas Gazdag, Jan-Philipp Stegho¨fer, Simon Daum, and Daniel Loebenberger. ”Migrating Software Systems towards Post-Quantum-Cryptography–A Systematic Literature Review.” arXiv preprint arXiv:2404.12854 (2024).

[7] Khan, Muhammad Asghar, Shumaila Javaid, Syed Agha Hassnain Mohsan, Muhammad Tanveer, and Insaf Ullah. ”Future-Proofing Se- curity for UAVs With Post-Quantum Cryptography: A Review.” IEEE Open Journal of the Communications Society (2024).

[8] Sharma, Purva, Anuj Agrawal, Vimal Bhatia, Shashi Prakash, and Amit Kumar Mishra. ”Quantum key distribution secured optical networks: A survey.” IEEE Open Journal of the Communications Society 2 (2021): 2049-2083.

[9] Shim, Kyu-Seok, Boseon Kim, and Wonhyuk Lee. ”Research on Quantum Key, Distribution Key and Post-quantum Cryptography Key Applied Protocols for Data Science and Web Security.” Journal of Web Engineering 23, no. 6 (2024): 813-830.

[10] Shim, Kyu-Seok, Yong-hwan Kim, Ilkwon Sohn, Eunjoo Lee, Kwang-il Bae, and Wonhyuk Lee. ”Design and validation of quantum key management system for construction of KREONET Quantum Cryptography Communication.” Journal of Web Engineering 21, no. 5 (2022): 1377-1417.