International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

A Verifiable and Efficient Symmetric Searchable Encryption Scheme for Dynamic Dataset with Forward and Backward Privacy

1. A. Pavan Teja, 2. K. Somashekhar, 3. M.L. Sudarshanreddy, 4.Y.Yaswanth,
5.A. Reddy Neela Assistant professor-Supervisor**.**
Department of mathematical Sciences, Mohan Babu University, India
E-Mail: pavantejarammurthi@gmail.com
Department of mathematical Sciences, Mohan Babu University, India
E-Mail: reddysudarshan877@gmail.com
Department of mathematical Sciences, Mohan Babu University, India
E-Mail: konganapadusomasekhar9@gmail.com
Department of mathematical Sciences, Mohan Babu University, India
E-Mail: yaswanth58@gmail.com

https://doi.org/10.55041/ijsmt.v2i4.433

Cite this Article: Teja, A. P., Somashekhar, K., Sudarshanreddy, M. & Y.Yaswanth, (2026). A Verifiable and Efficient Symmetric Searchable Encryption Scheme for Dynamic Dataset with Forward and Backward Privacy. International Journal of Science, Strategic Management and Technology, *02*(04). https://doi.org/10.55041/ijsmt.v2i4.433

Abstraction: Cloud storage has now become widely used for the management of sensitive documents, thereby casting a huge shadow over the user's right to privacy and the security of his data. One of the earliest encryption methods is AES, which is the most widely used among the rest of the traditional methods, and it still provides confidentiality only but not secure searching over the encrypted data. The new research introduces a QKD + AES-based Symmetric Searchable Encryption (SSE) system applicable to dynamic datasets and thus allowing secure keyword-based search without compromising the privacy. Under this scheme, QKD is the method used to send the AES encryption keys to the client and server securely, and thus the quantum adversaries cannot either intercept or manipulate the keys. After that, the AES encryption holds the data securely, while the SHA-256 hashing for the indexing of keywords is employed which allows an efficient and secure search over the encrypted data to be done. The system, besides giving forward privacy which forbids the connection of new data to previous searches, also provides backward privacy which assures that deleted entries will not be accessible in future queries. Moreover, the role-based access control mechanism is applied to permit

access with security based on such user roles as managers, finance staff, employees, and so on, along with their respective privileges. The proposed system not only guarantees an extremely high level of privacy protection but also provides very quick retrieval of the data thus being the ideal solution for the privacy-preserving cloud-based applications.

Keywords: Symmetric Searchable Encryption (SSE), Quantum Key Distribution (QKD), AES Encryption, SHA-256 Hashing, Forward Privacy, Backward Privacy, Role-Based Access Control, Secure Data Search, Cloud Security.

I.INTRODUCTION

The reliance on cloud storage for the storage and processing of sensitive organizational data has given rise to data privacy and security concerns that are of very high significance. One of the main benefits that cloud services offer is to be able to scale and to be cost-

effective, yet at the same time, they expose a lot of sensitive information to risk and this risk is mainly through various security threats especially when the data is in plaintext or poorly protected formats. Traditional encryption techniques like AES (Advanced Encryption Standard) do a great job in ensuring the data confidentiality but they also face the challenge of not being able to completely support keyword-based search queries over the encrypted data. The existing options do not allow either dynamic operations (like insertions and deletions, etc.) or they do not safeguard the privacy during these updates.

SSE (Symmetric Searchable Encryption) provides an extremely good and promising solution for encrypted data secure search as it allows the users to search for specific keywords without decrypting the entire dataset. However, still most of the SSE schemes are designed for static datasets and they often do not provide strong privacy throughout data updates. Furthermore, these schemes typically rely on complex techniques such as trapdoors or message authentication codes (MACs), which can result in the extra computation time thus reducing their scalability in real-world implementations.

The goal of the project is to eliminate these limitations through the utilization of Quantum Key Distribution (QKD) paired with AES encryption in an SSE setting. QKD is indeed to crypto methods what the warp drive is to spaceships, that is, a fast method of key distribution that is based on quantum physics to securely deliver the keys to the parties in communication. Therefore, no matter how powerful quantum computers become, the interception of the key exchange cannot be the outcome of any simulated monitoring. On top of that, AES assures lea\sing confidentiality of the data that is being transerred and SHA-256 hashing of the search terms provides a quick and secure indexing method for the search.

The system that is being developed will also assure users of their power to determine which future queries will be related to. This is done through the unlinking of fresh data to old queries and thus the garbage records, which are no longer needed, will be kept secure by being made inaccessible in future searches. In addition to this, the system will also have role-based access control (RBAC) integrated within it, giving managers, finance, and employees securely access to encrypted data according to their roles. QKD paired with AES encryption embodies the final aim of the project which is to develop a scalable, efficient, and privacy-preserving solution for searching encrypted data in cloud environments, which will be perfect for security and dynamic data operation applications.

A. Objective of the study

The project has been set up to realize a Quantum Key Distribution (QKD) + AES-based Symmetric Searchable Encryption (SSE) system that will make keyword-based search over encrypted data stored in the cloud to be both secure and efficient. The safe transfer of AES encryption keys through QKD between client and the server is the core of the project. No eavesdropping or hacking will be allowed in the distribution of the keys. Data encryption with AES will be applied to the most sensitive data and only those gaining the keys through QKD can decrypt this data. Besides, the project intends to apply SHA-256 hashing for the keyword indexing and thereby to apply searchable encryption to facilitate updates on the encrypted data without disclosing any sensitive information. The privacy of the system will be improved by the provision of forward privacy which will prevent the newly added data from being associated with the earlier searched data and backward privacy that will make it impossible for the deleted data to access by the future searches. The project also emphasizes the implementation of role-based access control (RBAC) for managing the access to encrypted data based on the user's roles such as managers, finance staff, and employees. This access control will ensure that only unauthorized users will be able to perform specific actions on the data. Additionally, the project will make an effort to find a lightweight and scalable solution that can quickly process data changes like insertions and deletions in a dynamic manner while still achieving high performance at a very low computational cost. The final milestone is to develop a data management system that would be compatible with the cloud, would not affect the privacy, and would be capable of meeting the strong security requirements along with the real-time performance at the same time.

B. Scope of the Study

The main objective of this initiative is to create a Quantum Key Distribution (QKD) + AES (Advanced Encryption Standard)-based Symmetric Searchable Encryption (SSE) system with a dynamic dataset, which will enable secure and efficient keyword-based search of encrypted cloud data. To put it simply, the project will carry out QKD to not only secure the key exchange but also AES keys will be securely distributed between the client and the server preventing the quantum adversaries from eavesdropping. The implementation of AES encryption on sensitive data will not only render it undetectable but also allow efficient keyword search through SHA-256 hashing-based meta-data indexing at the same time. Moreover, the system is going to manage the privacy concerns with keys and will provide forward privacy—which prevents new data from being connected to previous inquiries—and backward privacy—whereby deleted data is still inaccessible. Role-based access control will be among the factors of implementation which will limit access to data according to users' jobs like managers, accountants, and workers thus making data operations secure and controlled. The project is bringing a lightweight, scalable, and efficient solution that will be able to support dynamic operations like data adding and removing along with no security or performance compromise. The system is cloud-based still multi-keyword search or advanced cryptographic methods such as trapdoors or MACs will not be the features offered. In the end, the aim is to deliver a secure, efficient, and scalable system for privacy-preserving search over encrypted data in cloud-based applications, thereby solving the problem of data confidentiality and real-time usability at the same time.

C. Problem Statement

With companies adopting cloud storage as their primary method of keeping sensitive data, the privacy and security of such data have become the biggest concerns. Even though the most advanced encryption techniques, such as AES, are very effective in providing confidentiality, they also completely restrict the possibility of an efficient search on encrypted data. The contemporary Symmetric Searchable Encryption (SSE) schemes frequently fail to deliver forward privacy, which implies that new data can be associated with the previous queries and hence there is no backward privacy so that deleted data can be retrieved. Furthermore, many SSE systems rely on very intricate techniques, such as trapdoors or message authentication codes (MACs), which result in enormous computational effort. The aim of this project is to develop a QKD + AES- based SSE system that utilizes QKD to protect the exchange of AES keys for performing the keyword-based search over the encrypted data while ensuring both forward and backward privacy and eliminating the necessity for complicated cryptographic methods.

II. RELATED WORK

The secure storage and search of cloud data using Quantum Key Distribution (QKD) and AES encryption have been the main topic of research in recent times, partially because of the heightened expectations for privacy and security in the cloud environment. Combining QKD with AES encryption has been one of the methods that have been employed in the secure key exchange and protection of data which has also been using hash-based indexing (like SHA-256) for encrypted data search by keywords, thus granting data security and fast search capabilities [1]. A related system has been created which combines AES with Elliptic Curve Cryptography (ECC) for light-weight encryption wherein the keys are allocated and controlled based on role-based access rights thus making cloud file storage private [2]. Furthermore, cloud computing with encrypted data and homomorphic encryption models that allow secure computations have been proposed thus the privacy of the data is not compromised even during processing [3]. In the case of searchable encryption, advanced encryption schemes like AES + ECC have been applied for securing keyword-based searches over encrypted cloud data [4]. Role-based access control (RBAC) has been implemented to limit the access of sensitive information only to the authorized users; this, in turn, has led to secure cloud-based applications [5]. The cloud security sector has made significant strides by blending conventional encryption with quantum-safe measures such as QKD [6]. In addition, the combination of quantum cryptographic protocols and AES encryption has been investigated by the researchers to not only protect the cloud data but also allow for keyword search on encrypted content, thereby making the right trade-off between security and search efficiency [7]. The use of QKD and AES together as a hybrid encryption method for secure data sharing and

storage in cloud platforms has been suggested, which will consequently improve data confidentiality and access control [8]. Moreover, the concept of multi-layer encryption has been researched wherein QKD guarantees secure key distribution, and AES is used for data encryption, thus securing its storage and retrieval [9]. Another area of research has been the integration of quantum encryption with existing cloud security protocols and the consequent focus on security, data integrity, and search capabilities over encrypted datasets [10]. The evolution of quantum computing technologies has necessitated quantum-safe cryptography to become a prime concern in cloud data management, guaranteeing long-term security. It has been established that the use of quantum-safe key exchange (like QKD) together with symmetric encryption techniques such as AES can be an effective approach for cloud-based data storage and retrievals [11]. Recently, the cloud encryption frameworks have made further advancements by also providing role-based access control (RBAC) and dynamic updating (insertions and deletions) of the encrypted data which assures security and privacy during data operations [12].

III.PROPOSED SYSTEM

Their system proposal includes Quantum Key Distribution (QKD) plus AES-based Symmetric Searchable Encryption (SSE) technology. The transition will tremendously diminish privacy and security problems in cloud data management. QKD assures the delivery of the AES encryption keys through the secret channel and therefore the unhindered monitoring or capturing of the keys is not allowed, thus leading to security. Confidentiality of data will be mainly kept by AES encryption while SHA-256 hashing will be used for keyword indexing and thus making the search over the encrypted data efficient. The system is going to facilitate secure dynamic data operations even if they include insertions and deletions. Nonetheless, it will still uphold security. The system will provide forward privacy such that it will be hard to associate new data with the previous queries and backward privacy such that the removed records will not be available in the future searches. The system will also have role-based access control (RBAC) which allows different users like managers, finance staff, and workers to securely access data according to their roles and interact with it. This secure data search solution will not only be efficient and scalable but also strong privacy with real-time performance in cloud environments without the need for complicated cryptographic methods like trapdoors or MACs.

A. Overview of our work

The need for privacy and security of sensitive data has become a major hurdle to overcome as the usage of cloud storage is on the rise for such purpose. AES, a traditional encryption technique, ensures confidentiality of data but does not allow for secure search over an encrypted dataset during the whole life cycle of data, especially in cases where data is frequently changed or updated. On the other hand, Symmetric Searchable Encryption (SSE) has emerged as an effective technique allowing keyword-based search over encrypted data. However, one of the drawbacks of existing SSE schemes is that they handle dynamic data operations such as insertions and deletions with limited support, and they do not guarantee strong privacy such as forward and backward privacy.

This project introduces a solution that not only entangles Quantum Key Distribution (QKD) technology with AES-based Symmetric Searchable Encryption (SSE) but also it is a novel one. QKD plays an important role in securing the key exchange as it is not only secure but also impossible for the eavesdropper to detect, thus making the system quantum-proof. The data is encrypted by AES which keeps it confidential through the process of keyword categorization for security search over the data. The design of the application is capable of executing dynamic modifications and hence new data will not be provoked to past queries (forward privacy) and the data that has been erased will still be beyond access (backward privacy).

In addition to that, the system has a role-based access control (RBAC) as part of the system for security access with respect to user roles—managers, finance personnel, and employees—ensuring restricted access to sensitive data by only the users with authorization. The constructed system by combining QKD and AES is thus a scalable, efficient and privacy-preserving solution for encrypted-data search in cloud environments without the burden of complex cryptographic mac.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Project Flow

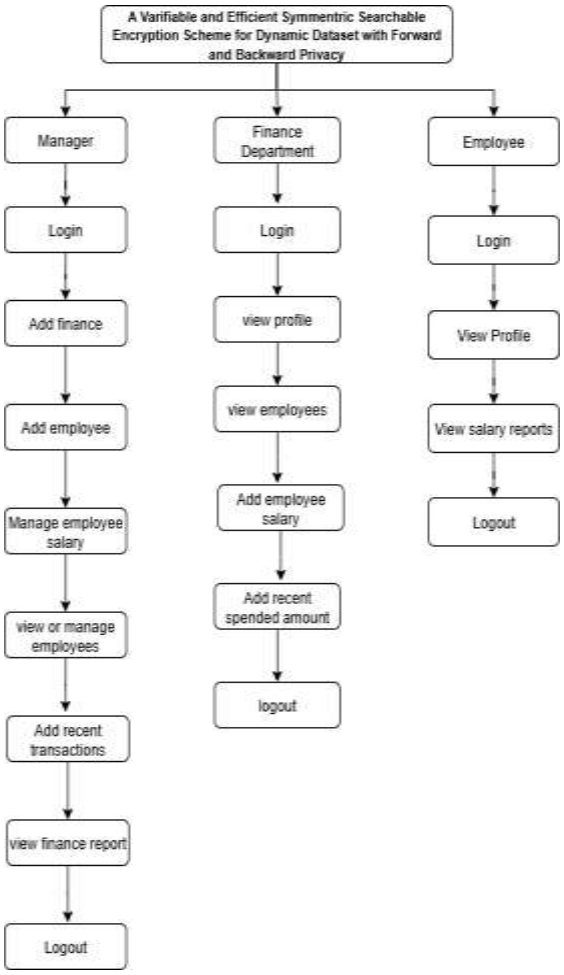

Figure 1 - Project Flow

Manager:

- **Add Finance Department:** The manager can add new finance department users by securely entering their details into the system.
- **Add Employee:** The manager can register employees and assign them to relevant departments.
- **Manage Salary:** The manager can create and update encrypted salary records for each employee.
- **View Finance Report:** The manager can securely view financial reports, which are protected using AES encryption.

Finance Department:

- **Add Spent Amount**: The finance user can record expenditure data, which is encrypted using AES before storage.
- **Manage Salary Records:** Can view and update employee salary details securely.
- **View Employee List:** Access a list of registered employees in the system for whom salary or expense data is managed.

Employee:

- **View Salary Reports:** Employees can log in and securely view their encrypted salary information.
- **Profile Access:** Employees can access their personal profile and verify data integrity.
- **Search Encrypted Data:** Employees can search over encrypted records (e.g., salary history) using hashed keywords (SHA-256).

IV. METHODOLOGY

Quantum Key Distribution:

QKD enables two users to definitively exchange cryptographic keys via a quantum channel, and it cannot be achieved by an eavesdropper to secretly exchange the key without the knowledge of any other party.

Mathematical Description of QKD:

1. Key Generation:

- Alice generates a random bit string $\{b1,b2,...,bn\}$ where each bit $bi \in \{0,1\}$.
- Alice then randomly chooses a basis for each bit. The basis $ki \in \{0,1\}$ indicates whether she will use the standard (rectilinear) basis or the diagonal basis for encoding the bit.

$bi=0 \rightarrow |0\rangle$
$bi=1 \rightarrow |1\rangle b\_i = 1$

- If Alice chooses the **diagonal basis** (basis 1)

bi=0→2|0⟩+|1⟩
bi=1→|0⟩−|1⟩2b_i = 1

2. Bob's Measurement:

- **Bob** also generates a random bit string for the measurement basis ki′∈{0,1}.
- Depending on ki′, Bob measures the incoming quantum bit:

If ki′=0,
If ki′=1,

- The measurement results in the **bit** bi′ for each bit that Bob receives. If Alice and Bob chose the same basis for a bit bi, the result bi′ will match bi . Otherwise, it will be random.

Key Generation:

- Once Alice and Bob have exchanged their bits, they reveal to each other the bases they have selected (but not the actual bits). They get rid of the bits that were based on different bases.
- The bits that are left over constitute the secret key which is shared by Alice and Bob and will be utilized for AES encryption.

Mathematical Formula for the Key Generation Process in QKD:

Let:

- BA={b1,b2,...,bn} be the bit string generated by Alice.
- KA={k1,k2,...,kn} be the basis string Alice uses for encoding the bits.
- BB={b1′,b2′,...,bn′} be the bit string received by Bob.
- KB={k1′,k2′,...,kn′} be the basis string Bob uses for measuring the bits.

The shared secret key is formed by:

K_{shared}={bi|ki=ki′}

Where bi corresponds to the bits where both Alice and Bob have chosen the same basis.

Advanced Encryption Standard:

AES is a symmetric key ciphering algorithm, a block of finite sized information mechanism. AES employs two substitution-permutation networks and works in round to change plaintext to a ciphertext.

Mathematical Description of AES:

The Advanced Encryption Standard is operable on 128-bit blocks of plaintext and employs either 128, 192, or 256 bits long keys. The method consists of a mix of operations like:

1. Initial Round (AddRoundKey)

- The plaintext P is divided into 4 words, each 32 bits long.
- The key K is also divided into 4 words of 32 bits each.
- The first round involves XORing the plaintext with the key:

P0=P⊕K

2. Rounds:

- **Sub Bytes**: An S-Box substitution table governs the substitution process and it is a non-linear process. The state is composed of bytes that are replaced by the S-Box values corresponding to them.

S′=S(S)whereS(x)∈S-Box

- **Shift Rows**: The rows of the state matrix are shifted cyclically.

ShiftRowi=Shift(Pi,i)
where i is the row number.

- **MixColumns**: Matrix multiplication over a finite field modifies the state matrix based on the previous column. GF(2^8).

Ci=M×Pi
where M is a fixed matrix, and Pi is the column vector.

- **AddRoundKey**: The current state is XORed with each round key deriving from the original expanded key.

Si=Si⊕Ki

- **Final Round:** The MixColumns step is exempted in the last cycle. At this stage, the final ciphertext C is expected.

C=FinalRound(P)

Working

The planned system combining QKD and AES-based Symmetric Searchable Encryption will be operating in such a way that first Quantum Key Distribution is utilized for the safe and secured exchange of AES encryption keys between the client and server through a quantum channel, thus ensuring the keys are absolutely and totally safe from interception. After the AES keys are successfully and securely exchanged, the AES encryption is applied to encrypt the sensitive data which is located in the cloud, thus providing the confidentiality of the data. In the case of the secure keyword-based search, the primary step is to apply SHA-256 to create a hash of the index of the data, enabling the user to search the encrypted data and at the same time the underlying plaintext is not being exposed. During the search process, the query is hashed and the server goes on to look for a match to the hashed query in the encrypted indices and the server decrypts the corresponding data with the AES key before sending the result back to the user. The system provides forward privacy, which implies that it will not be able to link newly added data to past searches, and backward privacy, which means that data that has been erased will not be retrievable in future searches. Furthermore, the system incorporates role-based access control (RBAC), which prevents access to data based on user roles such as managers, finance, and employees, thus making sure that only the authorized personnel can access the respective data. The system also supports dynamic transactions like adding and deleting of records, without the re-encryption of the entire dataset, which is very efficient for real-time cloud applications. To sum up, the union of QKD for secure key exchange combined with AES for data protection makes the system not only secure but also fast and capable of becoming a standard in the cloud environment.

V.RESULTS AND DISCUSSION

The results of the proposed system are provided here in the form of implementation screenshots.

A. User End Implementation Screenshots

The screenshots taken during the implementation of each stage of the proposed “A Framework for Cloud Based Fingerprint Authentication”.

Salary Management: Here, Manager can manage employee’s salary he accepts that time salary will be credited to employee, here manager can search employee with emp_id which is hashed in database.

Figure 1 - The screenshot of Employee Salary

Finance Dashboard: After login, Finance redirect to Finance dashboard.

Figure 2 - The screenshot of Finance Dashboard

VI.CONCLUSION

The proposal which combines QKD + AES-based Symmetric Searchable Encryption (SSE) system is the one that gives a strong and secure way to search through the encrypted data in the cloud and at the same time give a strong privacy guarantee. The combination of Quantum Key Distribution (QKD) for secure key exchange and AES encryption for data confidentiality protects the system from any attacks whether they are coming from classical or quantum sides. Not only does the system support dynamic data operations like secure insertion and deletion, but it also ensures both forward and backward privacy. Furthermore, role-based access control (RBAC) allows to assign data security and access according to the user's role, which provides an additional layer of security and usability. The clever use of SHA-256 hashing for indexing the keywords allows conducting extremely fast and highly secure search operations without exposing the plaintext data. This solution is elastic, light-weighted, and suitable for real-

time cloud environments, thus making it one of the strongest contenders for privacy-preserving applications in contemporary cloud infrastructures. The combination of the strong encryption of the system, support for dynamic data, and robust privacy features all together yield its viability for securing cloud data storage and retrieval against the continuously changing security challenges.

VII.FEATURE ENHANCEMENT

The QKD + AES-based Symmetric Searchable Encryption (SSE) system has the potential to magnitudes of improvement in the areas of functionality and security through the addition of some new traits. Let's start from the beginning, the system can let the users perform multi-keyword searches or give phrase-based queries which means the search over the already encrypted data becomes more and more flexible and accurate at the same time. The implementation of a tiny but strong MAC-based verification mechanism will be a great way of ensuring the integrity and completeness of search results, to the extent that the users will be able to spot and report any missing or altered records. Furthermore, the introduction of fuzzy keyword search would facilitate the processing of minor typographical errors or variations in the search terms, thus leading to the system being more user-friendly. Besides, for the sake of better monitoring and security, real-time access logging and alerting mechanisms could be added to the system for detecting suspicious activities and quick responding to potential threats. Moreover, the biometric authentication like fingerprint or facial recognition can be adopted during the user login stage for providing the highest security, thus rendering the sensitive data to be protected by an even stronger layer. Besides, the system can also incorporate cloud platforms such as AWS, Azure, Google Cloud, etc. for using the scalable encrypted storage which will make it possible to have both data and index structures securely backed up. Lastly, the setting up of a special admin and audit panel would not only make it easier to manage user roles, data access histories, and overall encrypted data operations monitoring, but also to increase the security and usability of the system.

VIII.REFERENCES

1. G. Vaddeswaram, "Advancing Quantum Cryptography Algorithms for Secure Data," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 15, no. 9, 2024. Available at IJACSA
2. S. Vasavi Venkata Lakshmi and Ziaul Haque Choudhury, "Secure Data Access in Cloud Environments Using Quantum Cryptography," arXiv:2506.10028 [cs.CR], June 2025. Available at arXiv
3. D. Dhinakaran, D. Selvaraj, N. Dharini, S. Edwin Raja, and C. Sakthi Lakshmi Priya, "Towards a Novel Privacy-Preserving Distributed Multiparty Data Outsourcing Scheme for Cloud Computing with Quantum Key Distribution," arXiv:2407.18923 [cs.CR], July 2024. Available at arXiv
4. Varsha Pravin Hole, Nikahat Mulla, and Pravin Basavraj Hole, "Effective Quantum Key Distribution Using Modified Key Sifting Scheme for Cloud Storage Security," International Journal of Intelligent Engineering and Systems, vol. 16, no. 2, 2023. Available at IJIES
5. Kari Elisabeth Larsen, Lars Magnus Johansen, and Olav Alexander Pedersen, "Quantum Cryptography for Enhanced Security in Cloud-Based Systems," International Journal of Electrical Engineering, Mathematics and Computer Science (IJEEMCS), vol. 1, no. 2, 2024. DOI: 10.62951/ijeemcs.v1i2.77. Available at IJEEMCS
6. Umer Nauman, Miaolei Deng, Uzair Salman, et al., "Q-ECS: Quantum-Enhanced Cloud Security with Attribute-Based Cryptography and Quantum Key Distribution," Journal Unknown

(2024-2025). Available at Semantic Scholar: Q-ECS

7. Arman Sykot, Md Shawmoon Azad, Wahida Rahman Tanha, BM Monjur Morshed, Syed Emad Uddin Shubha, and M. R. C. Mahdy, "Multi-Layered Security System: Integrating Quantum Key Distribution with Classical Cryptography to Enhance Steganographic Security," arXiv:2408.06964 [cs.CR], August 2024. Available at arXiv

8. Koushik Kumar Ganeeb, Vivekananda Jayaram, Manjunatha Sughaturu Krishnappa, Pankaj Gupta, Akshay Nagpal, Amey Ram Banarse, and Seema G Aarella, "Advanced Encryption Techniques for Securing Data Transfer in Cloud Computing: A Comparative Analysis of Classical and Quantum-Resistant Methods," International Journal of Computer Applications, vol. 186, no. 48, Nov 2024. Available at SSRN

9. Sebastian Verschoor et al., "A Critical Analysis of Deployed Use Cases for Quantum Key Distribution and Comparison with Post-Quantum Cryptography," EPJ Quantum Technology, vol. 12, Article number 51, 2025. Available at SpringerOpen

10. "Quantum Safe Cryptography and Security," ETSI White Paper, 2018. Available at ETSI

11. Anju Rani, Xiaoyu Ai, Aman Gupta, Ravi Singh Adhikari, and Robert Malaney, "Combined Quantum and Post-Quantum Security for Earth-Satellite Channels," arXiv:2502.14240 [cs.CR], February 2025. Available at arXiv

12. Gadde S., "Quantum-Resilient Cloud Data Protection: A Novel Model," Concurrency and Computation: Practice and Experience, Wiley (2025). Available at Wile.