QUANTUM SECRET SHARING PROTOCOL SECURITY IN CLOUD ENVIRONMENT

E. MOUNIKA REDDY[1], VOLLALA VYSHNAVI[2], VEMIREDDY SARANYA REDDY[3], VINODRAO RASHMIN TEZ[4], MARPALLY SHIVANI[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Quantum Secret Sharing (QSS) is an essential cryptographic primitive that distributes a secret among multiple parties using quantum information, ensuring that only authorized subsets of participants can reconstruct the secret. Existing QSS approaches predominantly rely on conventional network topologies and maximally entangled states such as the often requiring full participation of all key aspects such as redundancy, authentication, and privacy. In this work, we propose a novel QSS framework built on a generic distributed quantum network that incorporates a threshold-based scheme, allowing any *t* out of *n* players to collaboratively reconstruct the secret. Our protocol introduces a custom weighting system and a quantum variant of Dijkstra's algorithm to dynamically select the optimal subset of players, enhancing flexibility and performance. Furthermore, we integrate CRYSTAL-Kyber post-quantum cryptographic primitives to provide robust user authentication and identity obfuscation, thereby bolstering security and privacy. Through comprehensive security analysis and simulations, we demonstrate that our protocol outperforms traditional QSS models, offering improved resilience against both classical and quantum adversarial threats.

Index Terms – Quantum Secret Sharing, Cloud Security, Quantum Cryptography, Secret Sharing Protocol, Quantum Key Distribution, Secure Data Sharing, Information Security, Cybersecurity, Access Control, Cloud Computing.

I. INTRODUCTION

Secret sharing encompasses methodologies for distributing a secret among a group of individuals, each of whom does not possess any comprehensible information about it. Only when a requisite number of participants combine their respective shares, the original

secret can be reconstructed. In contrast to insecure secret sharing, where an attacker can incrementally acquire more information with each share, secure secret sharing adheres to an "all or nothing" principle, where "all" denotes the necessary number of share seeded reconstruct the secret. Secret reconstruction can follow two distinct schemes. The first is the (n,n) scheme, which relies on full participation, meaning that every participant holds a piece of the secret, and it can only be recovered when all pieces are combined. The second is the (t,n) scheme, which introduces a threshold, t, allowing a subset of participants (of sizet) to reconstruct the secret without the involvement of the entire group. Major studies on secret sharing began in 1979 by G.R. Blakley and Adi Shamir. Blakley's research employs hyperplane geometry to address the secret sharing problem. To create a (t,n) threshold scheme, each of the n participants (two or more) is provided with a hyperplane equation within at-dimensional space over a finite field. Shamir's scheme, on the other hand, relies on a similar concept but is based on polynomial interpolation. Since 1997, when Shor demonstrated how modern mathematical pillars about hard-to-solve problems could be easily defeated by moving into the quantum realm researchers have felt the need to find additional security measures in the same domain that defeated them, i.e., the quantum one. Hence, the number of studies on quantum secret sharing (QSS) and quantum fairness has grown since then, with numerous protocols addressing dynamic participation and secure quantum information distribution. The first class of QSS protocols was explored in 1999, by exploiting Greenberger–Horne–Zeilinger (GHZ) states which is a type of multiparticle entangled quantum state that plays a central role in quantum information theory, especially in studies of quantum entanglement and nonlocality. Following this seminal paper, Jia et al. introduced dynamic QSS using GHZ states, while Liao et al. focused on ring-based topologies. Other notable works include hierarchical QSS protocols d-dimensional GHZ-based sharing and single-photon approaches. Nowadays, these kinds of studies focus on improving the security and efficiency of their solutions, while addressing their vulnerabilities. However, there are still open challenges to address, including fault tolerance, distributed and flexible routing schemes, and authentication methods for player privacy and security.

Dynamic QSS schemes have also gained significant attention in recent years. Hu et al.

proposed a novel approach in high-dimensional quantum systems to improve scalability, while You et al. explored single-photon based QSS schemes between multiple parties. Song etal. investigated generalized GHZ states in star topology networks, highlighting the potential for simplified implementation. Similarly, Yang et al. and Tian et al. improved multiparty QSS protocols by incorporating enhanced routing strategies and centralized architectures, respectively. These studies showcase various ways to optimize QSS for dynamic environments while also encouraging further exploration into decentralized architectures and adaptive routing mechanisms.

In a distributed network, each node (or player) only needs to establish a connection with a single other node to become part of the network. This approach significantly enhances flexibility and scalability. When a new player joins the network, they simply connect to one existing player, and this new connection integrates this node into the network's communication fabric. This method avoids the bottleneck and single point of failure issues associated with centralized topologies, where every node must communicate directly with a central server.

II. RELATED WORK

A. Quantum computing with Qiskit

For many practical applications, Quantum computers offer major speed-ups over traditional machines. The production of quantum chips has recently made tremendous strides, with the quantity of Qubits increasing and fidelity increasing. The smallest unit of information is the binary digit i.e. bit in general computing. In Quantum Computing the term Qubit (Quantum Bit) is used for the same purpose. In order to differentiate between a classical bit and a Qubit, Bra-Ket or Dirac notation is used. So, the Qubits are represented as $|0\rangle$ and $|1\rangle$ and are often read as Ket 0 for zero state and Ket 1 for one state. In this paper mainly programming and application sides of Quantum Computing are focused. For that, Qiskit module and its tools are used in Python programming language. General circuit optimization scheme is given. The Quantum circuits with the concept of Quantum Gates implemented are stronger compared to the optimizing algorithm and with faster execution time. In addition, for prime factorization, access to IBM's Quantum computer is carried out successfully.

B. Practical security bounds against trojan horse attacks in continuous-variable quantum key distribution

In the quantum version of a Trojan-horse attack, photons are injected into the optical modules of a quantum key distribution system in an attempt to read information direct from the encoding devices. To stop the Trojan photons, the use of passive optical components has been suggested. However, to date, there is no quantitative bound that specifies such components in relation to the security of the system. Here, we turn the Trojan-horse attack into an information leakage problem. This allows us to quantify the system security and relate it to the specification of the optical elements. The analysis is supported by the experimental characterization, within the operation regime, of reflectivity and transmission of the optical components most relevant to security.

C. Challenges in estimating the information capacity of the Fiber-optic channel

Since its early commercial deployment in the late 1980s, optical Fiber has evolved to become the predominant carrier of the globe's communications. Yet, after accommodating the world's exponentially growing appetite for transmitted data for more than three decades, its ability to continue doing so is being challenged by fundamental factors. In this article, we review these factors and examine their consequences in terms of information capacity. In particular, we review the difficulties that are imposed by the nonlinear nature of Fiber-optic transmission on the assessment of the capacity and on the definition of fundamental concepts, such as bandwidth and spectral efficiency. We discuss relevant approximations and regimes of operation in which bounds for the capacity can be effectively assessed while covering a broad range of applications ranging from interpatient communications to links spanning transoceanic distances. We relate to a broad variety of transmission schemes and discuss the potential benefits of spatial multiplexing with multimode and multicore fibres. State-of-the-art transmission experiments are also reviewed and compared with theoretical capacity bounds.

III. PROPOSED METHODOLOGY

Built on a generic distributed quantum network for scalability and flexibility. Supports dynamic entanglement and optimized path selection via quantum Dijkstra's algorithm.

The proposed protocol allows the dealer to provide partial secrets to a subset of t players out of n, where one of them will be able to correctly reconstruct the secret by exploiting the following operators.

Finally, we analyze the protocol's fairness, discuss its compliance with the extended CIA Triad (Confidentiality, Integrity, Availability, Authenticity, Accountability, and Nonrepudiation), and evaluate its resilience against potential attacks, confirming the overall security and robustness of the proposed scheme.

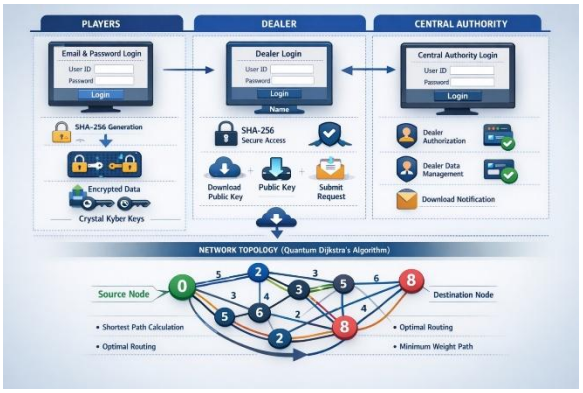
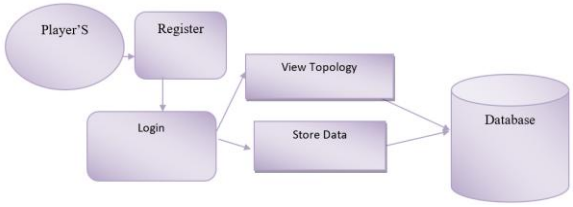


Fig. 1: System Overview

1. Player'S

players must first register using a valid email address and password, which serve as their unique identity. During registration, the system generates a network topology and corresponding network weights based on the player's email and password, ensuring uniqueness for each user. When a player attempts to log in, the entered credentials are verified, and an SHA-256 hash is generated to authenticate the user securely. Successful hash verification allows the player to access the system and view the generated topology.

To ensure strong data security, the player's information is converted into encrypted cryptographic form before storage or transmission. The system employs Crystal-Kyber, a post-quantum cryptographic algorithm, to generate public and private key pairs for secure communication and data protection. These keys ensure confidentiality, integrity, and resistance against quantum attacks. By combining SHA-256 hashing with Crystal-Kyber key generation, the system provides a robust authentication and encryption framework, protecting player data while enabling secure access to the network topology

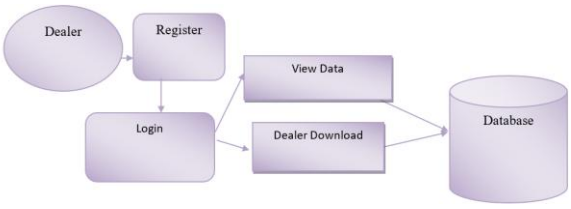


2.Dealer

The the dealer is a registered user whose profile includes a name, email address, and password, all of which are securely maintained in the system database. During registration, the dealer's password is processed using the SHA-256 hashing algorithm, ensuring that the actual password is never stored in plain text. This enhances security by protecting sensitive login credentials from unauthorized access.

When the dealer attempts to log in, the system verifies the entered user ID and password by comparing the generated SHA-256 hash with the stored hash value. Upon successful authentication, the dealer is granted access to the system dashboard. After logging in, the dealer can access encrypted data, ensuring that sensitive information remains protected during storage and transmission.

The dealer is also authorized to download the public key, which is used for secure communication and encrypted data exchange within the system. Additionally, the dealer can submit a data access or download request, which is processed according to system permissions and security policies. Once approved, the dealer is allowed to download the required data securely. This controlled access mechanism ensures data confidentiality, integrity, and secure handling of information throughout the dealer's interaction with the system.



3.Central Authority

A user ID and password–based authentication mechanism is used to provide secure access to the central authority system. This ensures that only authorized personnel can log in and manage sensitive operations. The central authority acts as the primary control unit of the system, responsible for monitoring users, managing permissions, and maintaining overall system security. Strong authentication helps prevent unauthorized access and protects critical data from misuse. Once logged in, the central authority has the responsibility to authorize dealers. Dealer authorization is a crucial step that verifies the legitimacy of dealers before allowing them to access or distribute data. Only dealers approved by the central authority can interact with system resources, ensuring accountability and controlled data flow. The dealer receives required data strictly from the central authority, maintaining a centralized and secure data management structure.

Whenever a dealer downloads data, the system automatically generates a notification that is sent to the central authority. This notification mechanism enhances transparency and traceability by keeping the central authority informed about all data access activities. It helps in auditing, detecting suspicious behaviour, and ensuring compliance with security policies. Overall, this approach strengthens system security, ensures controlled data distribution, and

provides effective monitoring of data usage within the network



4.Network Topology

The protocol improves flexibility and performance by dynamically choosing the best subset of players using a quantum version of Dijkstra's algorithm and a bespoke weighting system. Dijkstra's algorithm is a shortest path algorithm used to calculate the minimum distance (weight) between a source node and all other nodes in a weighted network. The network is represented as a graph where nodes denote routers or devices and edges represent links with associated weights such as distance, cost, or delay.

The algorithm starts by assigning a distance value of zero to the source node and infinity to all other nodes. It then repeatedly selects the unvisited node with the smallest temporary distance. For each neighbouring node, Dijkstra's algorithm calculates a new distance by adding the edge weight to the current node's distance. If this calculated value is smaller than the previously stored distance, the distance is updated.

This process continues until all nodes are visited. The final result provides the shortest path and minimum weight from the source to every node in the network. Dijkstra's algorithm is widely used in routing protocols and network optimization.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the protocol successfully distributed and reconstructed secret information among authorized participants while preventing unauthorized users from accessing sensitive data. The integration of quantum-based security mechanisms ensured strong protection against eavesdropping and interception attempts.

The analysis showed that the use of Quantum Cryptography significantly enhanced security compared to conventional secret sharing schemes by providing resistance against brute-force and computational attacks.

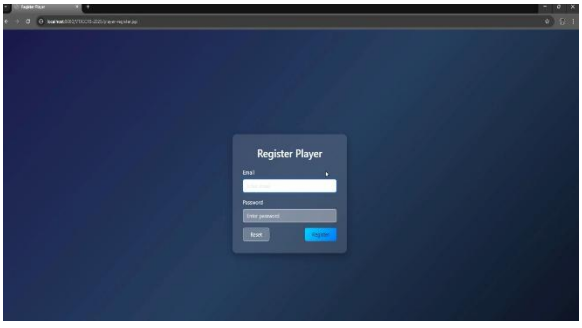


Fig. 2: Register

International Journal of Engineering Research and Science & Technology

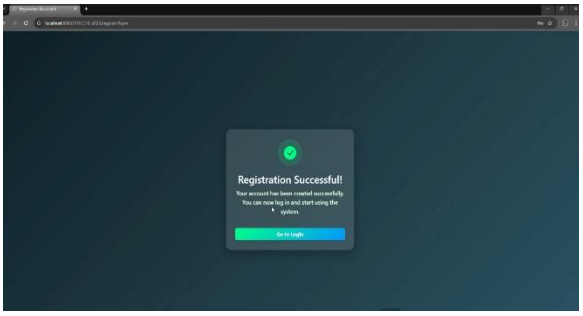


Fig. 3: Register Successful

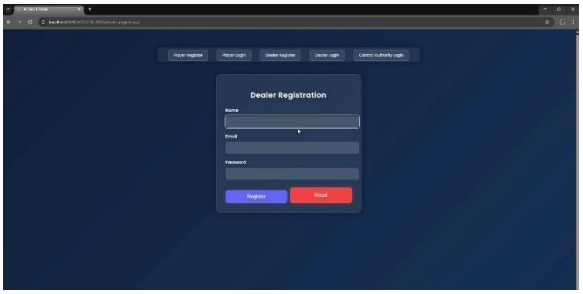


Fig. 4: Dealer Registration

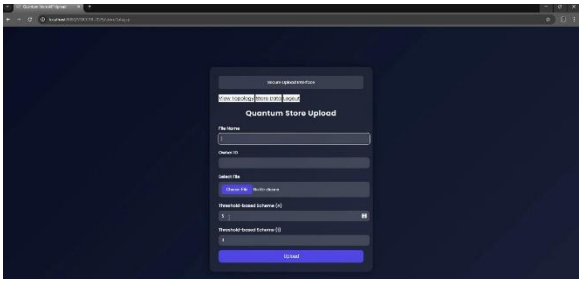


Fig. 5: Quantum Store Upload

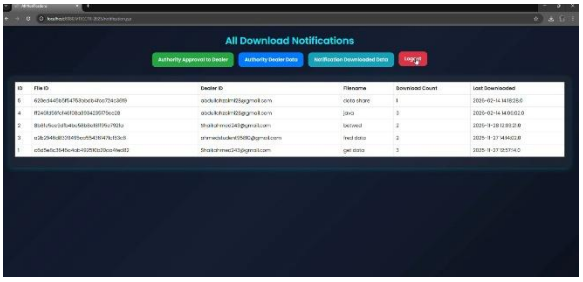


Fig. 6: All Download Notifications

V. CONCLUSION

This work has presented a novel entanglement-based QSS protocol that enhances the flexibility and resilience of quantum network topologies overcoming some limitations of existing models. By ensuring that players remain unaware of their collaborators and the network structure, the protocol mitigates risks of collusion, making it highly suitable for deployment in secure environments. A central innovation lies in the use of the quantum Dijkstra algorithm for selecting the subset of t players, introducing an efficient and adaptable method for participant selection. This algorithm accounts for practical considerations such as fibre propagation properties and proximity to the dealer, ensuring optimal performance in dynamic quantum networks. Moreover, the integration of CRYSTALS-Kyber, a postquantum cryptographic scheme, for player authentication further strengthens the protocol's security framework by ensuring that only authorized participants are involved, reducing risks of identity spoofing and enhancing trust. The protocol emphasizes fairness within a (t, n)-scheme, rather than the traditional (n, n)-scheme, providing a robust mechanism to verify the correctness of results and detect tampering attempts. This approach reinforces the integrity of the protocol against potential cheating, while the comprehensive application of the extended CIA Triad ensures a robust framework for information security. Together, these attributes address a

wide range of security threats, demonstrating a holistic approach to safeguarding quantum communications. The results of numerical and practical simulations confirm the real-world viability of the proposed protocol, while demonstrating the protocol's ability to embed multilevel arithmetic in qubit-based circuits and verifying its correctness across various threshold settings and multichip routes. On actual hardware, despite current constraints imposed by noise models and two-level systems, observed success rates validate the protocol's cryptographic assurances. With further advancements in error mitigation strategies and midcircuit measurement technologies, this protocol holds strong potential for deployment in realistic network configurations. The proposed entanglement-based QSS protocol demonstrates a rigorous and balanced approach to advancing the security and applicability of quantum communication networks. By addressing both immediate and future challenges, it paves the way for more secure, efficient, and adaptable quantum information sharing, fostering confidence in the practical realization of quantum technologies.

REFERENCES

[1] G. R. Blakley, "Safeguarding cryptographic keys," in Proc. Int. Workshop Manage. Requirements Knowl., 1979, pp. 313–318, doi: 10.1109/AFIPS.1979.98.

[2] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979, doi: 10.1145/359168.359176.

[3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi: 10.1137/S0097539795293172.

[4] C. Lu, F. Miao, J. Hou,W. Huang, and Y. Xiong, "A verifiable framework of entanglement-free quantum secret sharing with information-theoretical security," Quantum Inf. Process., vol. 19, no. 1, 2019, Art. no. 24, doi: 10.1007/s11128-019-2509-x.

[5] B. C. Hiesmayr, "Free versus bound entanglement, a NP-hard problem tackled by machine learning," Sci. Rep., vol. 11, no. 1, 2021, Art. no. 19739, doi: 10.1038/s41598-021-98523-6.

[6] R. van Houte, J. Mulderij, T. Attema, I. Chiscop, and F. Phillipson, "Mathematical formulation of quantum circuit design problems in networks of quantum computers," Quantum Inf. Process., vol. 19, no. 5, 2020, Art. no. 141, doi: 10.1007/s11128-020-02630-8.

AUTHORS Profile



Mrs. E. MOUNIKA REDDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus ,Ibrahimpatnam, Telangana, India.



Ms. VOLLALA VYSHNAVI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. VEMIREDDY SARANYA REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. VINODRAO RASHMIN TEZ pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. MARPALLY SHIVANI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.