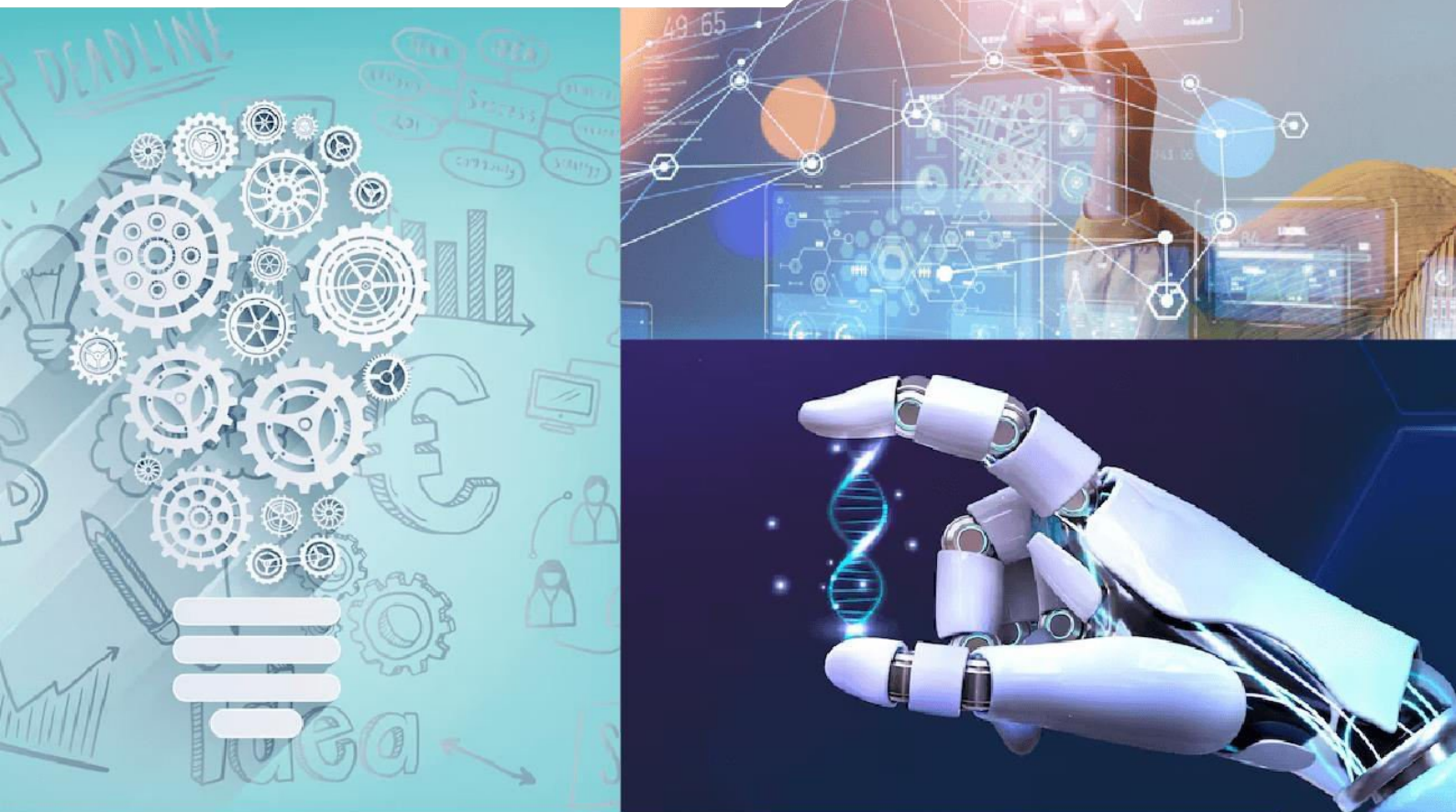




International Journal of Advanced Research in Education and Technology (IJARETY)

Volume 13, Issue 2, March - April 2026

Impact Factor: 8.152



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



An Advance Data Sharing with Quantum Secret Sharing Scheme with Cloud Data

Pravin Balu B¹, Katta Harshitha², Manda Keerthana³, Medipuri Nandini⁴

¹ Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India ^{2,3,4}

ABSTRACT: It is known that in certain quantum secret sharing schemes, participants may receive some shares before the dealer receives a secret. In the ramp quantum secret sharing schemes with the highest coding rate, it is unclear if some shares can be distributed prior to a secret being revealed. This article suggests methods for allocating some shares prior to disclosing a secret in those schemes. Since some participants may not be available when the dealer obtains the quantum secret, the new procedures expand the applicability of secret sharing schemes to broader scenarios. The correspondences between quantum secrets and quantum shares in the original schemes are then demonstrated to be preserved by our new encoding techniques, guaranteeing the retention of the original schemes' highest coding rates.

KEY WORDS

- **Quantum Secret Sharing (QSS):** A scheme for encoding a quantum state into multiple shares distributed among participants.
- **Ramp QSS (RQSS):** A variant allowing partial information leakage to unqualified sets to reduce share size.
- **Cloud Data Security:** The application of cryptographic techniques to protect data stored in distributed cloud environments.
- **Pre-Share Distribution:** A mechanism to distribute shares to participants before the final secret is known.
- **XOR-Based Encryption:** A symmetric encryption technique used to enhance data confidentiality within the system.

I. INTRODUCTION

The rapid expansion of digital data sharing has transformed how information is exchanged across healthcare, finance, and cloud-based platforms. However, this growth has also introduced significant risks regarding unauthorized access and data breaches. Standard encryption methods often fall short in complex cloud environments where data integrity and accessibility are paramount. Consequently, there is a critical need for advanced frameworks that not only secure data but also provide a managed, role-based environment for its distribution.

The proposed system addresses these challenges by integrating Quantum Secret Sharing (QSS) with robust cloud data management. By leveraging cryptographic techniques such as SHA-256 hashing for integrity and XOR-based encryption for confidentiality, the system ensures that sensitive information is protected from point-to-point. This architecture establishes a secure ecosystem involving Managed Service Providers (MSPs), administrators, and users, allowing for controlled access and verified data sharing that meets the security demands of modern digital infrastructures.

II. LITERATURE REVIEW

Secret sharing for cloud data security: A survey (2025) by V. Attasena, J. Darmont, and N. Harbi: This survey examines how secret sharing acts as a cryptographic technique to enforce data privacy, availability, and integrity in the "pay-as-you-go" cloud paradigm, even allowing for computation on encrypted data.

Strongly secure ramp secret sharing schemes for general access structures (2025) by M. Iwamoto and H. Yamamoto: This paper distinguishes between "strong" and "weak" ramp secret sharing (SS) schemes, noting that strong schemes are more desirable because they do not explicitly leak any part of a secret even if some information escapes from a set of shares.

Quantum strongly secure ramp secret sharing (2025) by P. Zhang and R. Matsumoto: This research introduces a quantum analog of classical strong security for ramp schemes. It demonstrates that while ramp schemes allow partial

information leakage to reduce share size, strong security ensures that qudits containing critical information remain protected.

Advance sharing of quantum shares for classical secrets (2025) by R. Miyajima and R. Matsumoto: This study proposes a quantum secret sharing method that allows for more flexible access structures and higher efficiency than classical methods. It specifically explores the capability of distributing certain shares before a secret is officially given.

Randomness cost of masking quantum information and the information conservation law (2025) by S. H. Lie and H. Jeong: This paper analyzes "quantum masking"—the process of encoding information into a bipartite state while forbidding local access—and provides a lower bound for the "randomness cost" required for this task based on information conservation laws.

The literature survey establishes that while secret sharing is vital for cloud data privacy and integrity, traditional methods struggle with efficiency in large-scale environments. It highlights the transition toward Ramp Quantum Secret Sharing (RQSS), which optimizes performance by balancing share size with strong security guarantees. The research underscores the necessity of "strong" security to prevent partial data leakage during the distribution of quantum information. Additionally, it identifies the importance of "pre-share distribution" to accommodate scenarios where participants are unavailable when a secret is first generated. Ultimately, the survey reveals a need for integrated systems that combine these quantum principles with robust, role-based access control for secure cloud storage.

III. METHODOLOGY OF PROPOSED SURVEY

The proposed methodology focuses on a role-based, secure cloud environment that integrates pre-share distribution in Ramp Quantum Secret Sharing (RQSS). The system is designed to provide high coding rates and ensure data confidentiality through a multi-modular approach.

System Overview

The system provides a secure, role-based cloud environment that integrates Ramp Quantum Secret Sharing to protect sensitive data with high coding efficiency. It features a unique pre-share distribution mechanism, allowing quantum shares to be allocated to participants even before the dealer receives the final secret. Security is reinforced through a layered approach, combining SHA-256 hashing for integrity and XOR-based encryption for data confidentiality. The architecture is managed through three distinct modules—Admin, MSP, and User—to ensure controlled access and streamlined data sharing across cloud infrastructures.

Working Process

1. **System Initialization:** The Administrator and Managed Service Provider (MSP) configure the cloud environment, verify user credentials, and define the quantum access structure (determining the number of participants needed to reconstruct the secret).
2. **Pre-Share Generation:** The dealer (MSP) prepares quantum ancillary states (qudits) in advance. These serve as the "foundation" of the secret before the actual data is even uploaded.
3. **Advance Distribution:** These prepared quantum shares are distributed to participants who are currently available. This allows the system to function even if some participants are offline when the final secret arrives.
4. **Secret Encoding & Classical Layering:** Once the user provides the secret, the dealer performs a local operation to bind it to the remaining shares. For added security, the system then applies XOR-based encryption and SHA-256 hashing to the data blocks.
5. **Storage & Reconstruction:** The secured data is stored in the cloud. To retrieve it, an authorized user provides a View Key, the system verifies data integrity, and a qualified set of participants combine their shares to reconstruct the original secret.

Modules of the System

Administrator Module: The central authority responsible for user authentication, approving registrations, and maintaining system integrity. It monitors the entire platform through detailed activity logs and manages overall security policies.

Managed Service Provider (MSP) Module: Acts as the technical "Dealer" in the quantum scheme. This module manages the cloud infrastructure, handles the generation and pre-distribution of quantum shares, and coordinates the secure storage of data blocks.

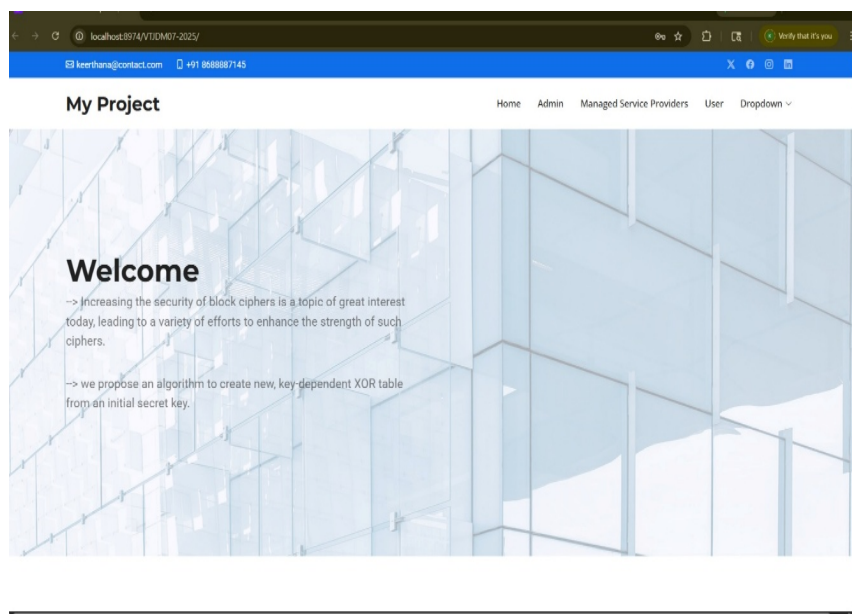
User Module: Represents the data owners and authorized recipients. Users can securely upload information to be converted into quantum shares, search for available data, and generate "View Keys" to authorize others to access or reconstruct their files.

System Benefits:

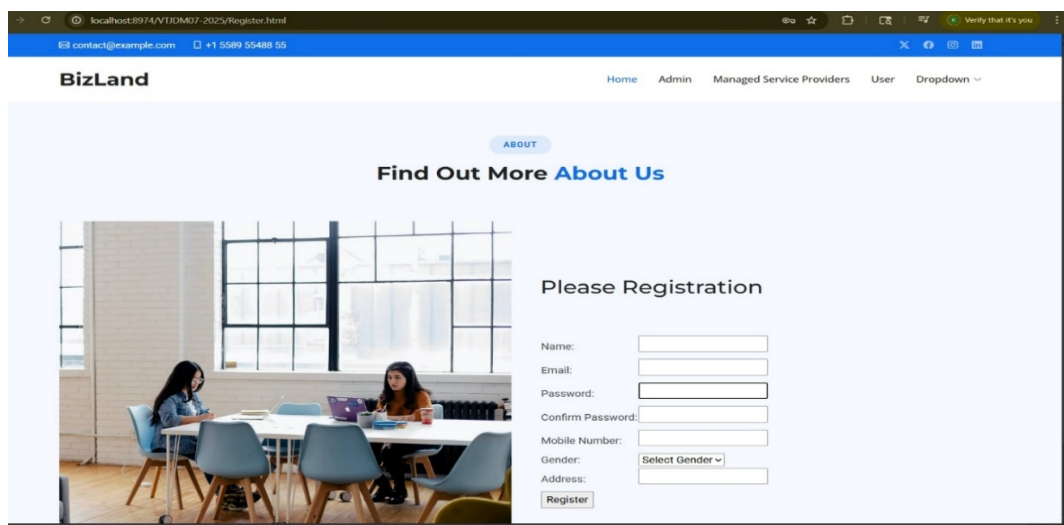
- Highest Coding Efficiency
- Enhanced Data Confidentiality
- Verified Data Integrity
- Scalability and Compatibility

IV. RESULTS

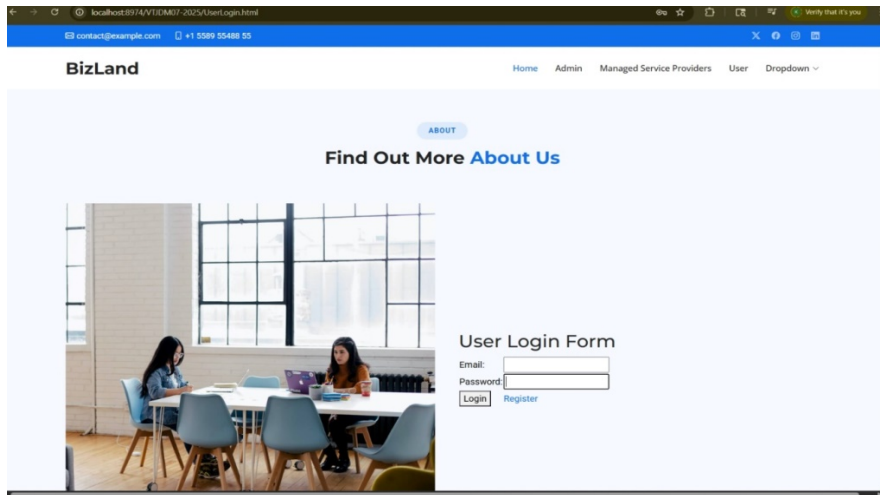
4.1 Home Page



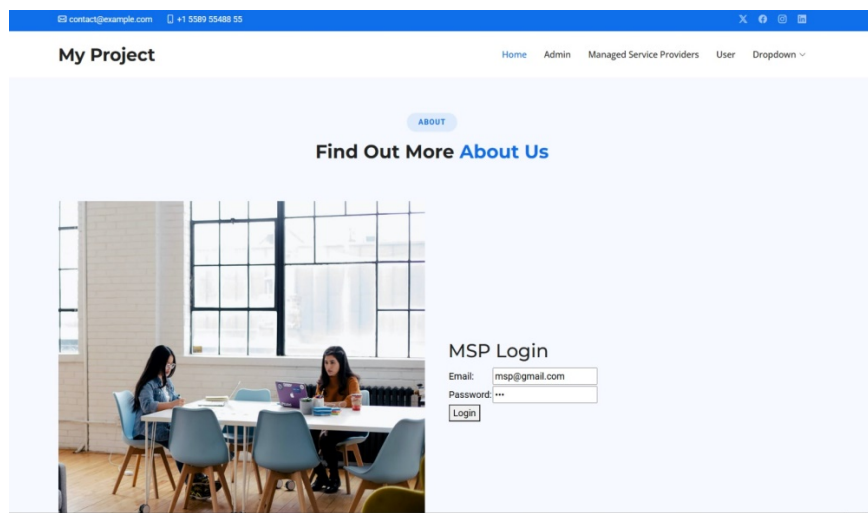
4.2 Registration Page



4.3 Login Page



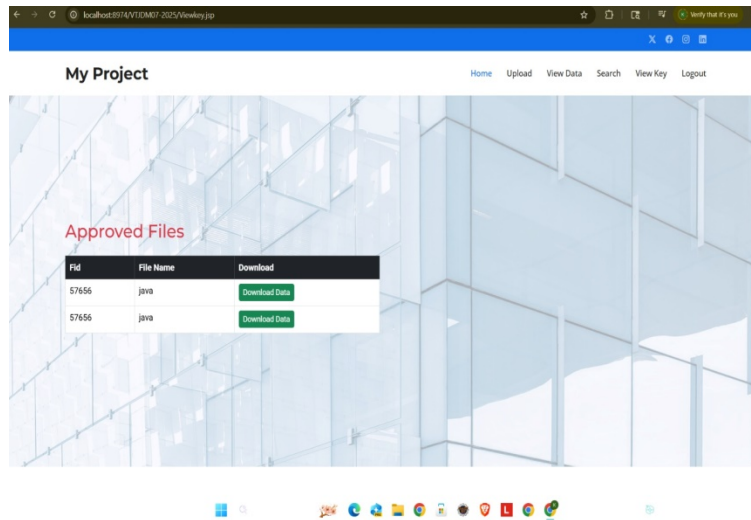
4.4 MSP login



4.5 Key Approval

MSP Panel		XOR Key Approval				
Home		File ID	File Name	User ID	Status	XOR Value
User Request		33898	Data	ibu@gmail.com	Approved	gMXOKIYjRNSqfg
XOR Key Request		98442	Java	keerthu89@gmail.com	Approved	qjpPhraqqzD00p
Logout		98442	Java	keerthu89@gmail.com	Approved	qjpPhraqqzD00p
		41897	Java	bunny9@gmail.com	Approved	qjpPhraqqzD00p
		50311	java	taju@gmail.com	Approved	qjpPhraqqzD00p
		57656	java	lucky@gmail.com	pending	pending
		57656	java	lucky@gmail.com	pending	pending

4.6 File Download



V. CONCLUSION AND FUTURE WORK

The system provides a secure cloud environment using Ramp Quantum Secret Sharing to protect data with maximum efficiency. It introduces a unique "Advance Sharing" innovation that allows quantum shares to be distributed to participants before the secret is even created. This pre-distribution ensures the scheme remains fully operational in real-world scenarios where some participants may be offline or unavailable during the final encoding phase.

Security is reinforced through a layered approach, combining SHA-256 hashing for integrity with XOR-based encryption for confidentiality. The architecture is organized into three distinct modules—Admin, MSP, and User—to ensure strict access control and clear operational accountability. Future enhancements may include integrating real quantum hardware and developing AI-driven threat detection to further protect the secret reconstruction process from potential breaches.

REFERENCES

- [1] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.
- [2] V. Attasena, J. Darmont, and N. Harbi, "Secret sharing for cloud data security: A survey," *Very Large Data Bases J.*, vol. 26, no. 5, pp. 657–681, Oct. 2017, doi: 10.1007/s00778-017-0470-9.
- [3] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, no. 3, pp. 648–651, Jul. 1999, doi: 10.1103/Phys-RevLett.83.648.
- [4] D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A*, vol. 61, no. 4, Mar. 2000, Art. no. 042311, doi: 10.1103/PhysRevA.61.042311.
- [5] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176.
- [6] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirements Knowl.*, Jun. 1979, pp. 242–269, doi: 10.1109/MARK.1979.8817296.
- [7] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," *Phys. Rev. A*, vol. 72, no. 3, Sep. 2005, Art. no. 032318, doi: 10.1103/Phys-RevA.72.032318.
- [8] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," *Inf. Process. Lett.*, vol. 97, no. 2, pp. 52–57, Jan. 2006, doi: 10.1016/j.ipl.2005.09.012.
- [9] H. Yamamoto, "Secret sharing system using (k, l, n) threshold scheme," *Electron. Commun. Jpn. I, Commun.*, vol. 69, no. 9, pp. 313–317, 1985, doi: 10.1002/ecja.4410690906.
- [10] P. Zhang and R. Matsumoto, "Quantum strongly secure ramp secret sharing," *Quantum Inf. Process.*, vol. 14, no. 2, pp. 715–729, Feb. 2015, doi: 10.1007/s11128-014-0863-2.
- [11] R. Miyajima and R. Matsumoto, "Advance sharing of quantum shares for classical secrets," *IEEE Access*, vol. 10, pp. 94458–94468, 2022, doi: 10.1109/ACCESS.2022.3204389

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 8.152