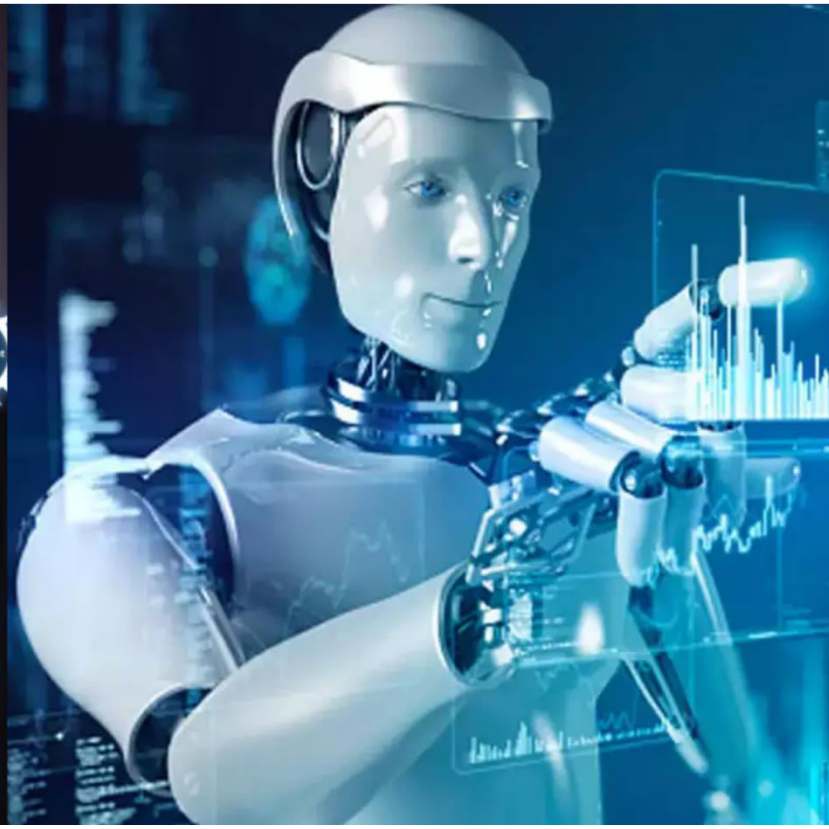
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411092|

A Secure and Efficient Proxy Re-Encryption Scheme for Secure Group Data Sharing in Cloud Computing: A Review

Dr Nilesh Mali, Ankita Prabhakar Istalkar

Department of Computer Engineering, Ajeenkya Dr D.Y. Patil School of Engineering and Technology Lohegaon, Pune, India

ABSTRACT: With the rapid development of cloud computing, organizations increasingly store and share massive amounts of data online. However, ensuring data confidentiality, access control, and untraceability during group data sharing remains a critical challenge. This paper proposes a **privacy-preserving and untraceable group data sharing scheme** that integrates **Proxy Re-Encryption (PRE)** and **Oblivious Random Access Memory (ORAM)** to achieve secure and efficient sharing among multiple users. The scheme introduces a novel **One-way Circular Linked Table (OCLT)** structure that conceals data access patterns, supports dynamic operations, and prevents tampering. Security analysis demonstrates resistance to collusion, tampering, and unauthorized access, while performance evaluations confirm lower computational and storage overhead compared to existing ORAM models.

KEYWORD: Cloud Computing, Privacy Preservation, Group Data Sharing, Proxy Re-Encryption, Oblivious RAM, Untraceable Data Access, Collusion Resistance, Access Control, Cryptography, Secure Cloud Storage.

I. INTRODUCTION

Cloud computing has revolutionized how data is stored and shared by offering scalability and cost efficiency. However, as data sharing in group environments (e.g., corporate, financial, or medical domains) increases, so do concerns regarding **data confidentiality** and **access traceability**. When multiple users interact with cloud-stored data, protecting against unauthorized access and hiding access patterns become essential. Traditional encryption methods fail to conceal data access sequences, allowing malicious servers to infer sensitive information.
To overcome these issues, this study integrates **proxy re-encryption** to facilitate secure key sharing among users and **ORAM** to ensure untraceable data access, thereby achieving an efficient, privacy-preserving multi-user data-sharing model in a cloud environment.

Motivation

1. **Increasing Dependence on Cloud Storage:** As organizations and users increasingly store and share data on cloud platforms, ensuring data security and privacy has become a major concern.
2. **Lack of True Privacy in Existing Systems:** Traditional encryption methods secure data but **fail to protect user access patterns**, allowing cloud providers or attackers to infer sensitive information through repeated access behaviors.
3. **Need for Multi-User Secure Sharing:** In real-world scenarios like finance, healthcare, and enterprise networks, **multiple users need to share and access common data** securely without risking exposure of confidential information.
4. **Vulnerability to Collusion and Tampering:** Semi-trusted cloud servers and malicious insiders can collude to tamper with or infer user data, creating a need for **collusion-resistant and tamper-proof mechanisms**.
5. **Efficiency and Scalability Requirements:** Existing privacy-preserving models often suffer from **high computational and storage overhead**, making them impractical for large-scale cloud environments.

II. LITERATURE REVIEW

Author(s): Masoomeh Sepehri, Alberto Trombetta, Maryam Sepehri
Title:*Secure Data Sharing in Cloud Using an Efficient Inner-Product Proxy Re-Encryption Scheme*
Year: 2018

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411092|

Description: Proposes an **Inner-Product Proxy Re-Encryption (IP-PRE)** method to allow flexible and secure data sharing in the cloud. It lets access policies be updated without re-encrypting data, enabling users to decrypt using their own keys. The scheme improves efficiency and ensures adaptive security under the Decisional Linear assumption.

Author(s): Kwame Opuni-Boachie Obour Agyekum, Qi Xia, Emmanuel Boateng Sifah, Christian Nii Aflah Cobblah, Hu Xia, Jianbin Gao
Title:*A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain*
Year: 2022
Description: Introduces a **blockchain-based proxy re-encryption framework** for secure IoT data sharing. Uses **edge devices** as proxies to offload computation and **information-centric networking** for efficient data delivery. Achieves decentralized, fine-grained access control ensuring confidentiality and integrity in IoT–cloud systems.

Author(s): Huidan Hu, Zhenfu Cao, Xiaolei Dong
Title:*Autonomous Path Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds*
Year: 2022
Description: Proposes a new **Autonomous Path Identity-Based Broadcast Proxy Re-Encryption (APIB-BPRE)** scheme enabling multi-hop transformation of decryption rights among multiple broadcast groups. This model supports flexible and efficient cloud data sharing while maintaining high security and practicality.

Author(s): Qinlong Huang, Wei Yue, Yue He, Yixian Yang
Title:*Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing*
Year: 2018
Description: Develops a **secure data sharing and profile matching scheme** for mobile healthcare social networks using **identity-based encryption**. Enables patients to share encrypted health records with doctors securely, perform privacy-preserving profile matching, and resist keyword guessing attacks while minimizing patient-side computation.

Author(s): Linmei Jiang, Donghui Guo
Title:*Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage*
Year: 2018
Description: Presents a **conditional proxy broadcast re-encryption** scheme supporting **dynamic user management** (add/remove users) without changing public keys. The cloud server can re-encrypt data directly for target users, improving sharing efficiency and maintaining data confidentiality and correctness.

Author(s): Linlin Xue
Title:*DSAS: A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System*
Year: 2022
Description: Proposes **DSAS**, a secure **proxy searchable re-encryption framework** for e-healthcare. It enables encrypted health record sharing with authorized doctors or institutions while allowing **search over encrypted data** and secure **delegation of medical research tasks**. Ensures privacy, confidentiality, and efficient remote access.

III. EXISTING SYSTEM

Existing cloud-based data-sharing schemes face significant limitations:

- **Single-user or one-to-one models** (e.g., classical proxy re-encryption) restrict sharing flexibility.
- **Attribute-Based Encryption (ABE)** supports access control but suffers from high computation costs and lacks scalability.
- **Tree ORAM** and **Path ORAM** techniques ensure access privacy but involve high communication overhead and limited efficiency.
- Existing systems cannot simultaneously guarantee **multi-user collaboration**, **untraceable data access**, and **tamper detection**.
- These drawbacks necessitate a more secure, scalable, and efficient solution that supports dynamic group membership and resists collusion.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411092|

IV. PROPOSED SYSTEM

The proposed scheme introduces a **privacy-preserving and untraceable group data-sharing mechanism** based on **Proxy Re-Encryption (PRE)** and **OCLT-ORAM**.

Key components include:

1. **Proxy Re-Encryption (PRE):**
- Enables secure data sharing among multiple users.
- Uses a multiparty key exchange protocol based on **Elliptic Curve Cryptography (ECC)** and **Bilinear Diffie–Hellman (BDH)** assumption to prevent collusion.
2. **OCLT-ORAM Structure:**
- A novel **One-way Circular Linked Table (OCLT)** embedded in a binary tree structure that hides access patterns.
- Supports dynamic operations such as data upload, download, and deletion with minimal computation cost.
3. **Access Control and Tamper Resistance:**
- Prevents revoked or malicious users from accessing shared data.
- Detects data tampering through hash verification within each block.
4. **Lazy Obfuscation Algorithm:**
- Dynamically updates data addresses with low computation, reducing server overhead.
5. **Fault Detection and Collusion Resistance:**
- Identifies and revokes malicious users and prevents server-user collusion.

This hybrid scheme ensures data privacy, access pattern hiding, collusion resistance, and efficient computation — all critical for real-world cloud data sharing applications.

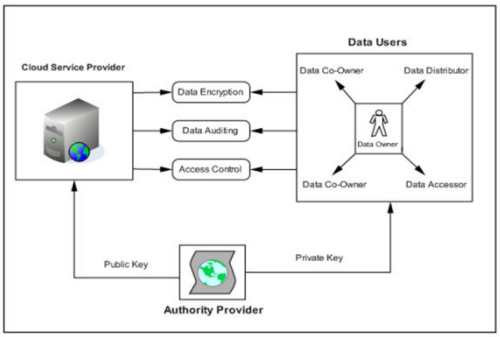


Figure 1. System Architecture

V. MATHEMATICAL MODEL

The mathematical model -
S={s, e, X, Y,Φ}
Where,
s = Start of the program.
1. Log in with webpage.
2. Load Files on cloud.
e = End of the program.
Retrieve the file from cloud storage system.
X = Input of the program.
Input should be File.
Y = Output of the program.
File will be first uploaded then search and send key and download the file
X, Y ∈ U
Let U be the Set of System.
U= {GM,GU, S, G, D}
Where GM,GU , F, S, T, M, D are the elements of the set.
GM=Group Manager
GU=Group User
S=Search keyword
G=Get key from user
D=Download file using key

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411092|

VI. CONCLUSION

The proposed privacy-preserving and untraceable data-sharing scheme successfully achieves secure multiparty collaboration in cloud environments. By combining **Proxy Re-Encryption** and **OCLT-ORAM**, it ensures both data confidentiality and untraceable access patterns. The system efficiently resists collusion, detects tampering, and supports dynamic user management while maintaining low computational and storage overhead. Security and performance analyses confirm that the scheme is both secure and scalable, making it a strong candidate for deployment in corporate, financial, and healthcare data-sharing applications.

REFERENCES

1. M. Sepehri, A. Trombetta, and M. Sepehri, "Secure Data Sharing in Cloud Using an Efficient Inner-Product Proxy Re-Encryption Scheme," Journal of Cyber Security and Mobility, vol. 7, no. 4, pp. 373–398, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/11048791/
2. K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," IEEE Systems Journal, vol. 16, no. 1, pp. 1685–1696, Mar. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9442931/
3. H. Hu, Z. Cao, and X. Dong, "Autonomous Path Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds," IEEE Access, vol. 10, pp. 78965–78979, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9862958/
4. Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing," IEEE Access, vol. 6, pp. 3657–3668, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8403204/
5. L. Jiang and D. Guo, "Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage," IEEE Access, vol. 5, pp. 17511–17519, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7979495/
6. L. Xue, "DSAS: A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System," IEEE Access, vol. 10, pp. 38191–38205, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9718101/

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details