UNTRACEABLE AND SECURE GROUP DATA SHARING IN PROXY SERVER

T.Mangaiyarthilagam[1], M.J.Dharaneesh[2],J.Hariprasath[3], T.Priyadharshini[4],R.Sheela[5]

Selvam College of Technology (Autonomous), Namakkal, Tamil Nadu, India.

1. Abstract

With the development of cloud computing, the great amount of storage data requires safe and efficient data sharing. In multiparty storage data sharing, first, the confidentiality of shared data is ensured to achieve data privacy preservation. Second, the security of stored data is ensured. That is, when stored shared data are subject to frequent access operations, the server's address sequence or access pattern is hidden. Therefore, determining how to ensure the untraceability of stored data or efficient hide the data access pattern in sharing stored data is a challenge. By leveraging proxy re-encryption and oblivious random access memory (ORAM), a privacy-preserving and untraceable scheme is proposed to support multiple users in sharing data in cloud computing. On the one hand, group members and proxies use the key exchange phase to obtain keys and resist multiparty collusion if necessary. The ciphertext obtained according to the proxy re-encryption phase enables group members to implement access control and store data, thereby completing secure data sharing. On the other hand, this paper realizes data untraceability and a hidden data access pattern through a one-way circular linked table in a binary tree (OCLT) and obfuscation operation. Additionally, based on the designed structure and pointer tuple, malicious users are identified and data tampering is prevented. The proposed scheme is secure and efficient for group data sharing in cloud computing. This project also enhanced Traitor Tracing Once the user's secret key is leaked for profits or other purposes, server runs trace algorithm to find the malicious user. After the traitor is traced, user will blocked in cloud server. The traceability function enables the broadcaster to identify the traitor, and prevents the authorized users from leaking their keys.

Keywords:

Untraceability, Proxy Re-encryption,Key exchange,Group data sharing.

2. INTRODUCTION

Cloud computing with low cost and convenient sharing of resources enables computing to be distributed among a large number of distributed computers, which has attracted the interest of many scholars. The computing resources for computing and processing data are provided by cloud computing. Moreover, the core of using many computing resources is to store and manage the data. That is, cloud storage is a cloud computing system with data storage and management as its core, which makes group data sharing possible. The security of data in group data sharing encounters two challenges when data are stored in a cloud server. On the one hand, the confidentiality of data is ensured during user interaction to preserve data privacy. Specifically, for practical applications such as a smart home network or a smart medical network, it is desirable to use a distributed computing platform to select a many-to-many sharing mode to share information within a group. Therefore, the data of multiple users in the group can be accessed by other users. However, the confidentiality of data needs to be guaranteed to prevent collusion or stealing of data in data sharing during data transmission. On the other hand, the address sequence or access pattern of the data is guaranteed to be not leaked when the shared data are stored in the server. In the server, an address sequence is generated corresponding to the data. Even if the user has encrypted the data, the curious server can infer the content of the address sequence with a higher probability when the user accesses the same or similar ad- dress sequence multiple times. Furthermore, the curious server may infer the importance of the encrypted data based on the number of times the address sequence was accessed to explore some of the private data.

3. MAIN SECTION- I

3.1 EXISTING SYSTEM

- Data sharing in cloud computing can be utilized in many fields to solve some difficult problems, but it also brings about some security issues. On the one hand, it is difficult to ensure the confidentiality of the ciphertext to preserve data privacy.
- Moreover, group data sharing in a many-to- many mode is a challenge. Additionally, the address sequence of the outsourced data stored in the server is easily monitored, or the access pattern of the data is easily determined.
- The cloud cannot hide the path of data stored in the server during data sharing, and a malicious user may trace the sequence of addresses of data, but some problems cannot resist collusion attacks and encounter difficulty in revoking malicious users.

Problem identified from the existing system:

1. Confidentiality of Ciphertext and Data Privacy Issues

- Ensuring the confidentiality of **encrypted data** is challenging, as unauthorized access can lead to data breaches.
- Existing encryption mechanisms may not be sufficient to **fully protect sensitive information** from sophisticated attacks.

2. Challenges in Many-to-Many Group Data Sharing

- In a **many-to-many** data-sharing environment, multiple users need access to shared data, making access control complex.
- Unauthorized access can occur if an **effective key management** system is not in place.
- Managing dynamic user groups (adding and revoking users) without **re-encrypting the entire dataset** is difficult.

3. **Address Sequence and Access Pattern Vulnerability**

- The cloud server cannot fully **hide the path of stored data**, making it possible for **attackers to monitor address sequences**.
- A **curious server** may analyze access patterns to infer **critical data insights**, even if the data itself is encrypted.
- Repeated access to the same **data block** may allow adversaries to determine the **importance or sensitivity of information**.

4. **Malicious User Tracking and Collusion Attacks**

- Malicious users may **trace the sequence of addresses** to infer confidential information.
- Some existing methods fail to **prevent collusion attacks**, where multiple attackers collaborate to breach security.
- Revoking malicious users efficiently **without disrupting legitimate users** is a challenge

Data sharing in cloud computing offers many advantages, such as enabling seamless collaboration and solving complex problems, but it also introduces significant security concerns. One of the main challenges is ensuring the confidentiality of encrypted data, as it's difficult to guarantee that only authorized users can access and decrypt it. Group data sharing, particularly in many-to-many scenarios, is complex and raises issues like improper access control, making it hard to secure. Additionally, the cloud system allows the tracking of data access patterns and the sequence of data addresses, which can be monitored by attackers, potentially compromising data privacy. Cloud systems also struggle to hide the path that data takes during sharing, allowing malicious users to trace these paths and exploit vulnerabilities. Moreover, even with strong security measures, collusion attacks, where multiple malicious users cooperate, can bypass protections. Revoking access from these malicious users is also a difficult task, leaving the system vulnerable to ongoing threats. These challenges highlight the need for robust and evolving security measures to ensure safe and private data sharing in cloud environments.

The Conclusion part of the existing system:

In conclusion, while data sharing in cloud computing enhances collaboration and problem-solving, it also presents critical security risks. Challenges such as ensuring data confidentiality, managing access control in group sharing, preventing data access pattern tracking, and mitigating collusion attacks make secure sharing complex. To address these issues, continuous advancements in security protocols are essential to safeguard data privacy and maintain trust in cloud environments.

4. MAIN SECTION- II

3.1 PROPOSED METHODOLOGY

1. Research Design

The study will adopt a structured research design to systematically investigate the core objectives. A combination of qualitative and quantitative approaches will be employed to ensure comprehensive analysis and accuracy in results. The qualitative approach will help in understanding subjective experiences and contextual factors, while the quantitative approach will provide measurable and statistical validation of findings. The research will follow an exploratory and descriptive design to ensure in-depth understanding and clarity on key issues.

2. Data Collection Methods

Primary Data:

- Surveys will be distributed among targeted respondents to collect structured data regarding opinions, experiences, and behaviors.
- Interviews will be conducted with key stakeholders to gather in-depth insights and qualitative perspectives.
- Questionnaires will be designed with both open-ended and closed-ended questions to ensure a balanced mix of quantitative and qualitative data.

Secondary Data:

- A thorough literature review will be conducted using peer-reviewed journals, books, and industry reports.
- Financial records and documents from the provided report will be analyzed to supplement primary data.

- Case studies of similar projects or organizations will be examined to draw comparisons and derive best practices.

3. Data Analysis Techniques

Qualitative Analysis:

- Thematic analysis will be used to identify patterns, themes, and key insights from interview transcripts and open-ended survey responses.
- Coding techniques will be applied to systematically categorize and analyze qualitative data.

Quantitative Analysis:

- Statistical tools such as regression analysis, correlation analysis, and descriptive statistics will be applied to analyze numerical data.
- Trend analysis will be conducted to assess financial patterns and performance over time.
- Financial modeling will be employed to predict future trends based on historical data.

4. Validation and Reliability

- To ensure credibility, cross-validation techniques such as triangulation will be used, comparing multiple data sources and methods.
- Reliability tests, including Cronbach's Alpha, will be applied to assess the internal consistency and reliability of survey instruments.
- Pre-testing of questionnaires and interview guides will be conducted to refine data collection tools before full-scale implementation.
- Any inconsistencies in data will be reviewed and resolved through expert consultation and secondary source verification.

5. Ethical Considerations

- All data collection activities will adhere to ethical guidelines to protect the rights and confidentiality of respondents.
- Participants will be informed about the purpose of the study and their consent will be obtained before data collection.
- Data sources will be properly cited to maintain academic and professional integrity and avoid plagiarism.
- Anonymization techniques will be applied where necessary to ensure respondent privacy and data protection.

6. Implementation Framework

The methodology will be executed in a systematic and phased approach:

- **Phase 1: Preliminary Data Collection and Literature Review**
  - Identifying relevant literature and financial reports.
  - Reviewing past studies, reports, and existing methodologies.
  - Refining research questions and hypotheses.
- **Phase 2: Conducting Surveys and Interviews**
  - Designing and pre-testing survey instruments.
  - Administering surveys and conducting structured interviews.
  - Collecting and organizing raw data.
- **Phase 3: Data Processing and Analysis**
  - Cleaning and structuring the collected data for analysis.
  - Applying qualitative and quantitative analytical methods.
  - Interpreting patterns and drawing meaningful conclusions.
- **Phase 4: Interpretation of Results and Documentation**
  - Synthesizing findings to address research objectives.
  - Preparing final documentation and reports.
  - Providing recommendations based on data insights.

This methodology ensures a structured, comprehensive, and reliable approach to achieving the research objectives effectively. It integrates both qualitative and quantitative techniques, adheres to ethical standards, and follows a phased implementation plan for systematic execution.

3.2 SYSTEM IMPLEMENTATION

HARDWARE REQUIREMENTS

Processor	: I3
Hard Disk	: 500 GB.
Monitor	: 15'' LED Monitor
Input Devices	: Keyboard, Mouse
RAM	: 4 GB.

SOFTWARE REQUIREMENTS

Operating system	: Windows 10
Coding Language	: ASP.NET,C#.NET
Front End	: Visual Studio 2008
Database	: SQL SERVER 2005

SOFTWARE RESULT:

- The developed software system offers a secure and efficient solution for multi-user data sharing in cloud computing environments. It integrates **proxy re-encryption** to allow encrypted data to be shared among group members without exposing plaintext to intermediaries, ensuring robust access control. To further enhance privacy, the system employs **Oblivious RAM (ORAM)**, which effectively hides

users' data access patterns, preventing the cloud server from tracing their behavior. A novel **one-way circular linked table (OCLT)** embedded in a binary tree structure is introduced to achieve untraceability and obfuscate access paths, enhancing both security and performance.

- The software also features a **pointer tuple mechanism** that enables the identification of malicious users and prevents data tampering by monitoring unauthorized changes. Furthermore, it includes a **traitor tracing algorithm** that detects when a user leaks their secret key, allowing the system to trace, identify, and block the offending user from future access. This traceability function ensures accountability among users and discourages key leakage. Additionally, the system is designed to resist **multi-party collusion**, strengthening overall security in group environments. As a result, the proposed software offers a comprehensive and reliable framework for privacy-preserving, untraceable, and secure group data sharing in the cloud.
- In addition to its core functionalities, the software ensures **scalability and efficiency**, making it suitable for real-world deployment in large-scale cloud environments. The **key exchange phase** is carefully designed to facilitate secure communication among group members and proxies, ensuring that encryption keys are distributed without risk of interception or misuse. This process not only enhances overall system integrity but also plays a crucial role in resisting collusion attacks where multiple parties may attempt to compromise the system.

- The integration of **proxy re-encryption** allows users to delegate access rights without revealing their private keys or requiring re-encryption of the entire dataset, thus reducing computational overhead. Meanwhile, the **ORAM mechanism**, in conjunction with the OCLT structure, allows frequent data access while effectively concealing access patterns, which is a critical feature for protecting user behavior and usage trends from being exploited by third parties or cloud providers.
- Moreover, the system includes a **behavioral monitoring component** that actively analyzes user access logs and pointer interactions to flag unusual patterns indicative of malicious intent. When anomalies are detected, the system can initiate automated security protocols, such as temporarily suspending user access or launching the **traitor tracing process**. If a key leak is confirmed, the system uses this mechanism to locate the source of the leak and enforce sanctions such as permanent account revocation or access denial, thereby preserving the integrity of the data-sharing network.
- By combining advanced cryptographic techniques with intelligent data structures and access monitoring, the system achieves a high level of **data confidentiality**, **access privacy**, **user accountability**, and **operational resilience**—all of which are essential for trustworthy cloud-based collaboration.

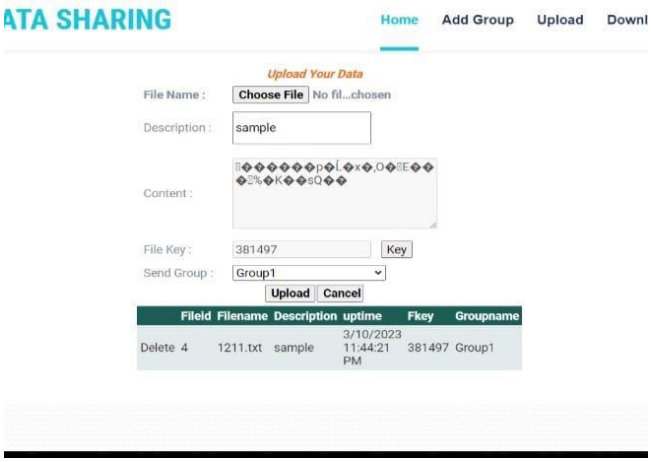
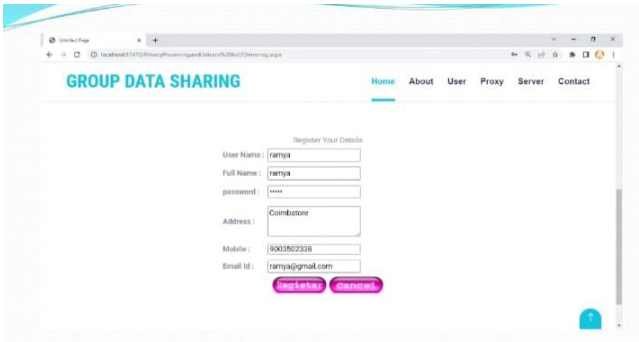


Fig 6: Generating Primary Key

Collectively, these results demonstrate that the software is not only capable of managing secure data sharing among multiple users but also adept at defending against a wide range of internal and external security threats



5. Conclusion

In this project, we present a secure and untraceable protocol for group data sharing in a cloud storage scheme. Based on key exchange, the proposed approach can efficiently generate the users conference key, which can be used to protect the security of shared data and prevent malicious user collusion with other users. In addition, security of shared group data in the cloud and access control is achieved with respect to the encryption technique. The sufficient security proof indicates the security of our protocol. The experimental comparison results could be considered as validation of the performance of our protocol, making it substantially more convincing.

REFERENCES

[1] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud stor- age auditing with key-exposure resistance," Information Forensics and Security, IEEE Transactions on, vol. 10, no. 6, pp. 1167–1179, 2015.

[2] R. S. Bali and N. Kumar, "Secure clustering for efficient data dis- semination in vehicular cyberphysical systems," Future Generation Computer Systems, pp. 476–492, 2016.

[3] S. Zarandioon, D. D. Yao, and V. Ganapathy, "K2c: Cryptographic cloud storage with lazy revocation and anonymous access," in International Conference on Security and Privacy in Communication Systems. Springer, 2011.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in 2010 proceedings ieee infocom. IEEE, 2010.

[5] M. Ali, R. Dhamotharan, E. Khan, S. Khan, A. Vasilakos, K. Li, and A. Zomaya, "Sedasc: Secure data sharing in clouds," IEEE Systems Journal, vol. 11, no. 2, pp. 395–404, 2017.

[6]S. Gordon, X. Huang, A. Miyaji, C. Su, K. Sumongkayothin, and K. Wipusitwarakun, "Recursive matrix oblivious ram: An oram construction for constrained storage devices," IEEE Transactions on Information Forensics and Security, vol. 12, no. 12, pp. 3024–3038, 2017.

[7] X. Chen, X. Huang, J. Li, J. Ma, W. Lou, and D. S. Wong, "New algorithms for secure outsourcing of large-scale systems of linear equations," IEEE transactions on information forensics and security, vol. 10, no. 1, pp. 69–78, 2014.

[8] H. Yuan, X. Chen, J. Li, T. Jiang, J. Wang, and R. Deng, "Secure cloud data deduplication with efficient re-encryption," IEEE Trans- actions on Services Computing, 2019.

[9] X. Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, "Lattice-based proxy-oriented identity-based encryption with key- word search for cloud storage," Information Sciences, vol. 494, pp. 193–207, 2019.

[10] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ecc-based provably secure three- factor user authentication and key agreement protocol for wireless healthcare sensor networks," Computers & Electrical Engineering, vol. 69, pp. 534–554, 2018.

[11] H. Yang, W.Zheng,T. Zhou,X. Jin, and A. Wang,"A privacy-pro tecting and resource-saving scheme for data sharing in smart home," J. Internet Technol., vol. 20, no. 2, pp. 607–615, 2019.

[12] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment," IEEE Internet Things J., vol. 5, no. 6, pp. 4900–4913, Dec. 2018.

[13] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, "Certificateless public key authenticated encryption with key word search for industrial Internet of Things," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3618–3627, Aug. 2018.

[14] M. Zhang, Y. Jiang, Y. Mu, and W. Susilo, "Obfuscating re-encryp tion algorithm with flexible and controllable multi-hop on untrusted outsourcing server," IEEE Access, vol. 5, pp. 26 419–26 434, 2017.

[15] A. Chakraborti, A. J. Aviv, S. G. Choi, T. Mayberry, D. S. Roche, and R. Sion, "rORAM: Efficient range ORAM with O (log2 N) locality," in Proc. Netw. Distrib. Syst. Secur. Symp., 2019.

[16]S. K. Haider and M. van Dijk, "Flat ORAM: A simplified write only oblivious RAM construction for secure processors," Cryptog raphy, vol. 3, no. 1, 2019.