e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

PRIVACY-PRESERVING AND UNTRACEABLE GROUP DATA SHARING SCHEME IN CLOUD COMPUTING

A Vinson*1, D.C Christo Melbin*2

*1Master Of Engineering, Computer Science And Engineering, CSI College Of Engineering, Near Ooty, Ketti, The Nilgiris, Tamil Nadu, India.

*2Assistant Professor, Department Of Computer Science And Engineering, CSI College Of Engineering, Near Ooty, Ketti, The Nilgiris, Tamil Nadu, India.

DOI : https://www.doi.org/10.56726/IRJMETS45050

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: Cloud Computing, Group Data Sharing, And Secret Key.

I. 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 [1] [2]. 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 [4]. The security of data in group data sharing encounters two challenges when data are stored in a cloud server [5]. 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 [6].

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.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

II. METHODOLOGY

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 cipher text 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.

Drawbacks:

It is still vulnerable under collusion attacks and revoked malicious users. The scheme is designed only for a general one-to-many communication system, which makes it inapplicable for the many-to-many pattern. This scheme suffers from the collusion attack performed by the cloud server and the revoked malicious user.

Proposed Methodology:

The proposed system, the data sharing more efficient and convenient. Our solution should try to satisfy the user's access to the data, rather than operating on data in a single manner. Specifically, users in a group can read, and upload data, and multiple users can perform access operations on data of multiple users. Second, the confidentiality of data should be ensured in the data sharing process to protect private data. The outsourcing data are the company's financial data, transaction data, etc.; the proposed scheme is secure and efficient for group data sharing in cloud computing. Moreover, our scheme ensures that business data can be securely transmitted in the channel, protecting the privacy of the data. The traceability function enables the broadcaster to identify the traitor, and prevents the authorized users from leaking their keys.

Block diagram:

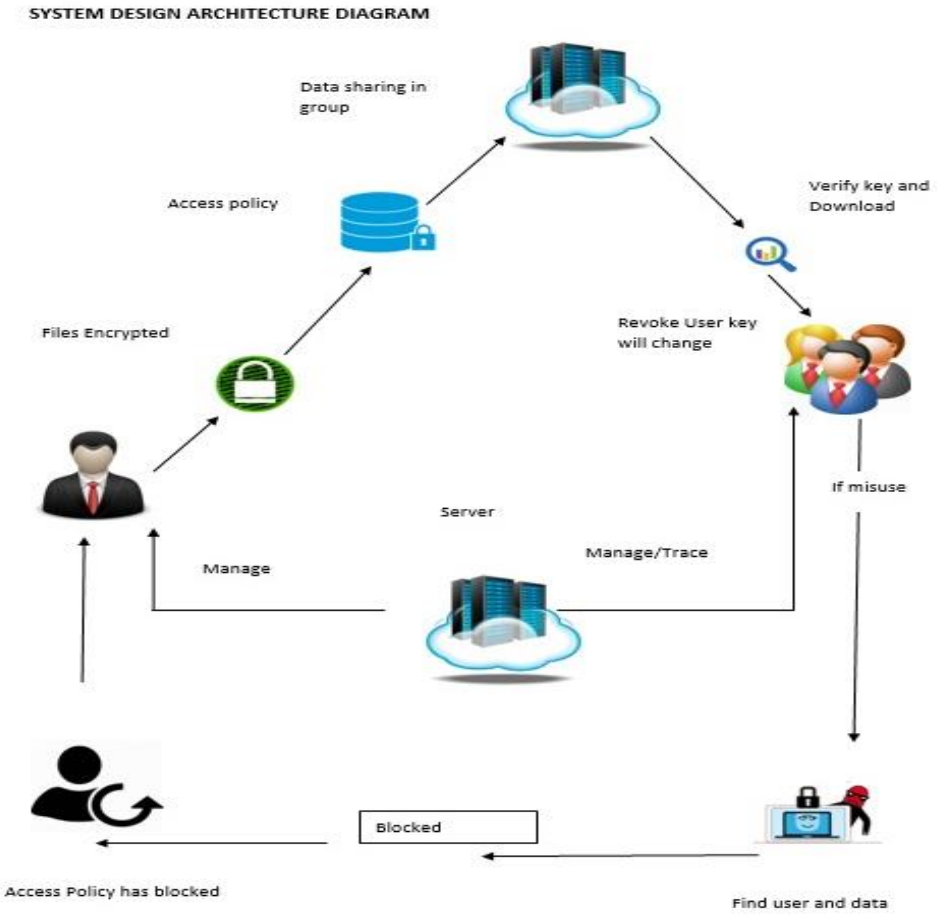

Figure 1: Block Diagram

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

Modules:

1. Users
2. Proxy
3. Cloud server
4. Data Security
5. Access Control
6. Traitor Tracing

Module Description

Users

In our proposed scheme, users are people who have contact with money and transaction data and who hope to share data. Moreover, the proxy is considered as a user, and the proxy joins in the key agreement phase. The reasons why the proxy is designed as a user are as follows. Two worrisome problems that occur when users access data in the cloud server are confidentiality of business data and computation of encryption data. Our proposed scheme utilizes characteristics of the OCLT structure to discern malicious users and then achieve user revocation to ensure the credibility of users in the same group.

Proxy

As a secure and trusted server in the company, the proxy is in charge of generating subkeys and sum keys, storing the index table with the data position information and distinguishing malicious users. The proxy in our proposed scheme is a key distribution center and fully trusted by both group users and the cloud server.

Cloud server

In this scheme, the cloud server is a semi-trusted entity. It has the characteristics of curiosity but honesty and provides users and the proxy with sufficient storage resources and computation and quality data sharing services. In other words, the cloud will not deliberately.

Data security

Encrypted outsourced data cannot be understood by servers and illegal users when sharing data in the cloud. To reduce the falsification probability of the key and the computational complexity of the proxy, our scheme should support re-encryption in the proxy so that data are re-encrypted prior to transmission to the cloud. In proposed system we using AES algorithm for data encryption.

Access control

The most concerning problem when sharing data is to ensure the access rights and security of users when group users dynamically change. Thus, users dynamically changing and access control should be sup- ported in our scheme. In other words, a joining user can share all existing data in the group, whereas a revoked user cannot retrieve group shared data in the cloud.

Traitor Tracing

Once the user's secret key is leaked for profits or other purposes, proxy runs trace algorithm to find the malicious user. After the traitor is traced, proxy sends user revocation request to cloud server to revoke the user's search privilege. The traceability function enables the broadcaster to identify the traitor, and prevents the authorized users from leaking their keys.

Advantages

The proposed scheme can efficiently support dynamic changes of users with respect to the access control and the many-to-many data sharing pattern. Consequently, users can safely exchange data with others under the semi-trusted cloud. Moreover, users can exchange information in the cloud anonymously with respect to the group signature. The proposed scheme is suitable for data sharing in a group manner under the cloud environment. Meanwhile, it can prompt the further development and employment of key agreement for data sharing.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

III. MODELING AND ANALYSIS

Data Flow Diagram

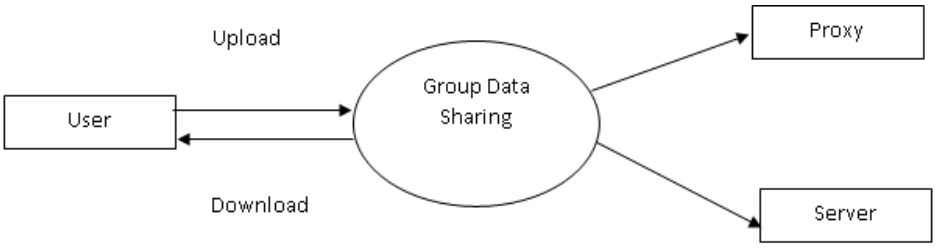

Figure 2: Data Flow Diagram (Level 0)

Data Collection

The practice of obtaining information from numerous sources is known as data collection.

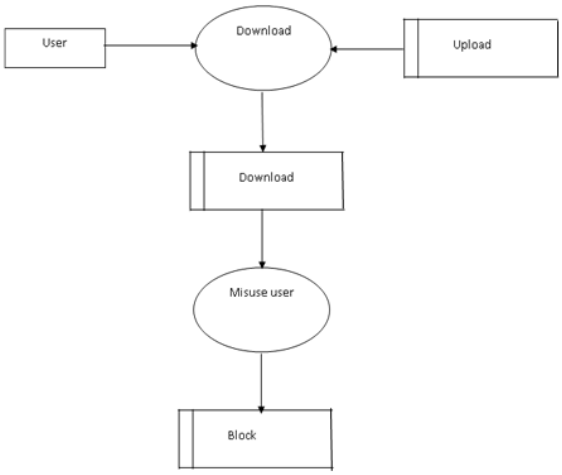

Figure 3: Data Flow Diagram (Level 1)

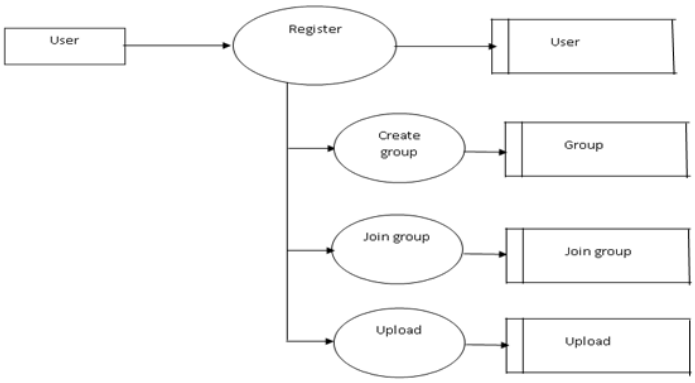

Figure 4: Data Flow Diagram (Level 2)

Input Design

Input design is the process of converting user-originated inputs to a computer-based format. Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system. Input design is a part of overall design, which requires careful attribute. Inaccurate input data are the most common cause of errors in data processing. The goal of designing input data is to make data entry as easy, logical and free from errors. In the system design phase input data are collected and organized in to groups of similar data.

Output Design

Output design generally refers to the results and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application. Computer output is the most important and direct source of information to the user. Output design is very important phase because the output will be in an interactive manner. The output will be in such away that the user can see it from the screen and can take a hard copy from the printer. Efficient, Major form of the output is a hard copy from the printer.

Database Design

Database design is the process of producing a detailed data model of a database. This logical data model contains all the needed logical and physical design choices and physical storage parameters needed to generate a design in a Data Definition Language, which can then be used to create a database. A fully attributed data model contains detailed attributes for each entity. In an object database the entities and relationships map directly to object classes and named relationships. However, the term database design could also be used to apply to the overall process of designing, not just the base data structures, but also the forms and queries used as part of the overall database application within the database management system.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

Implementation

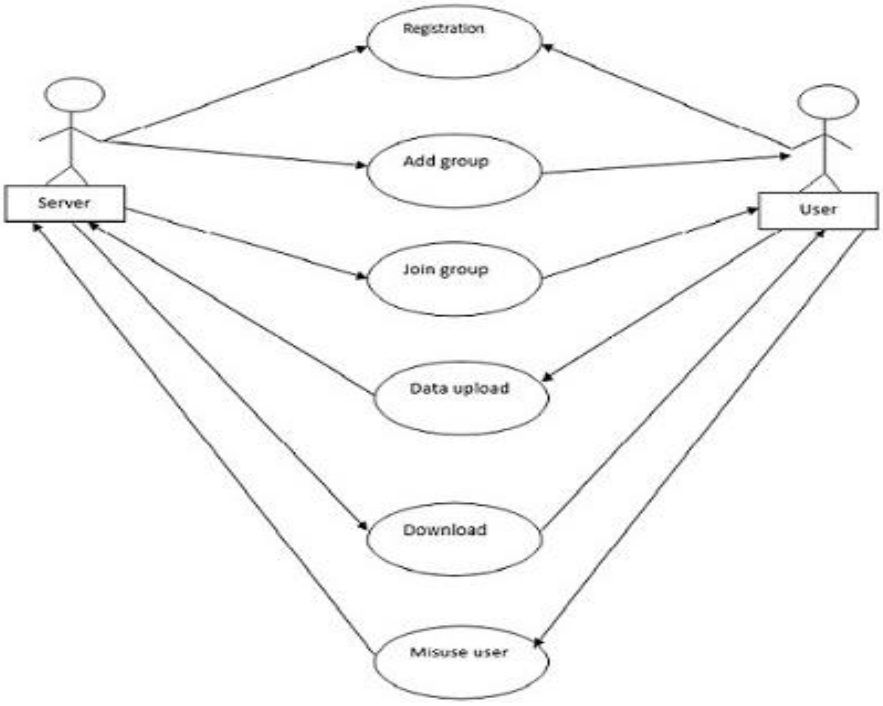

Fig 5: Use Case Diagram

Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is effective and workable. Implementation of this project refers to the installation of the package in its real environment to the full satisfaction of the users and operations of the system.

Testing is done individually at the time of development using the data and verification is done the way specified in the program specification. In short, implementation constitutes all activities that are required to put an already tested and completed package into operation. The success of any information system lies in its successful implementation.

System Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the user that it will work efficiently and effectively. The existing system was long time process. The project execution was checked with live environment and the user requirements are satisfied. Proper implementation is essential to provide a reliable system to meet the organization requirements.

IV. RESULTS AND DISCUSSION

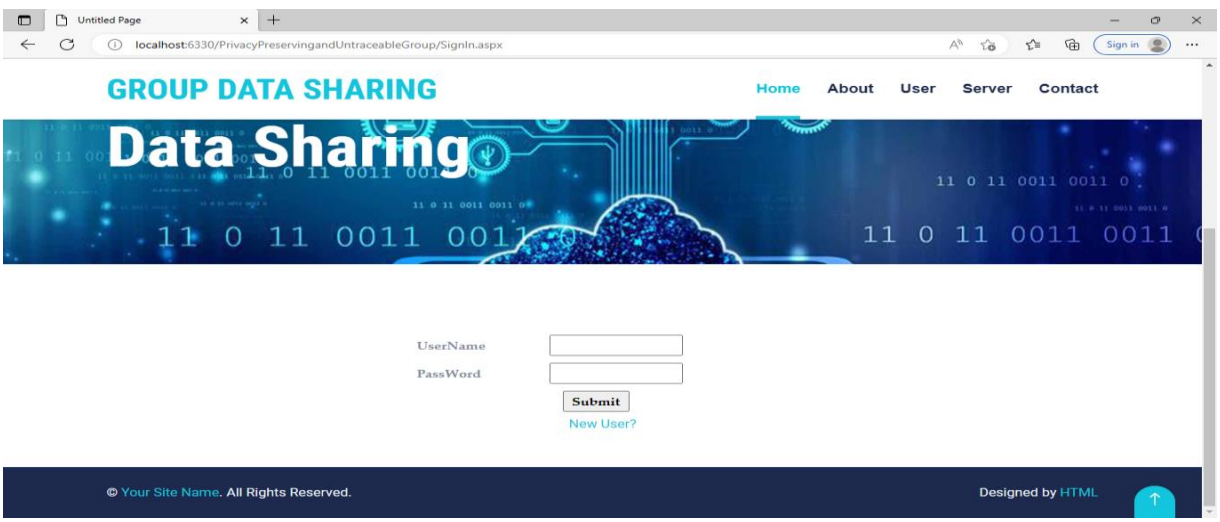

Fig 6.1: Login Page

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

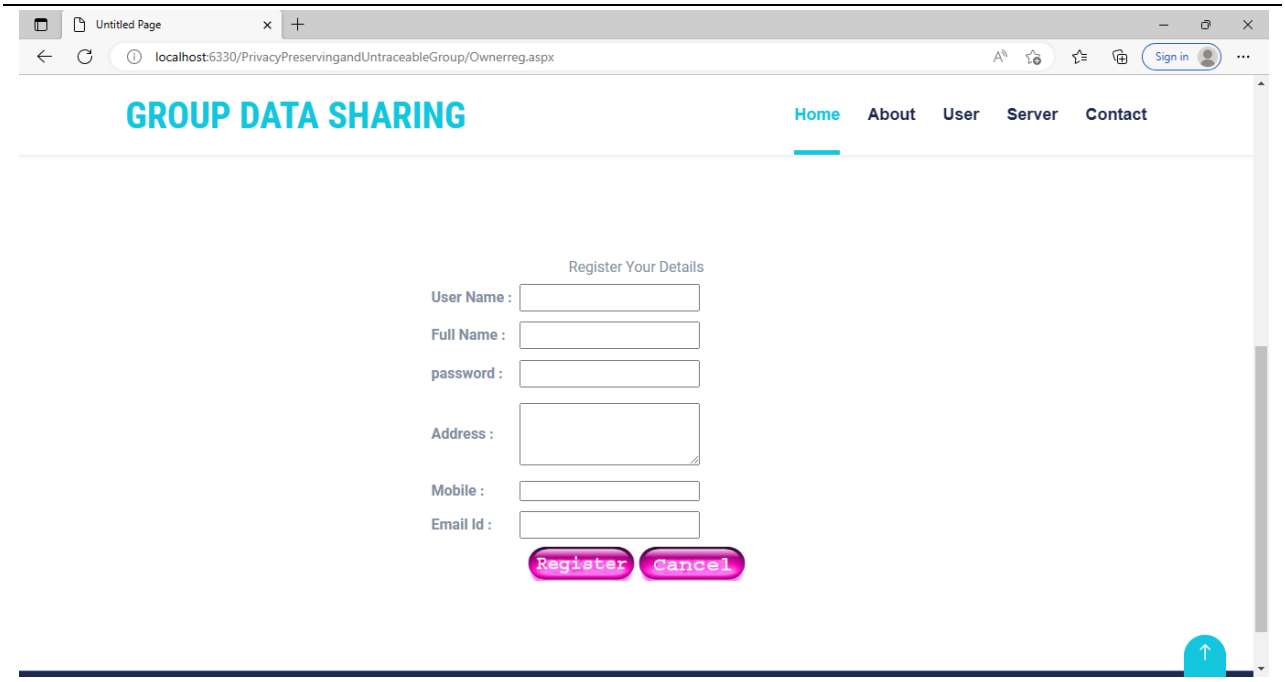

Fig 6.2: Register Page

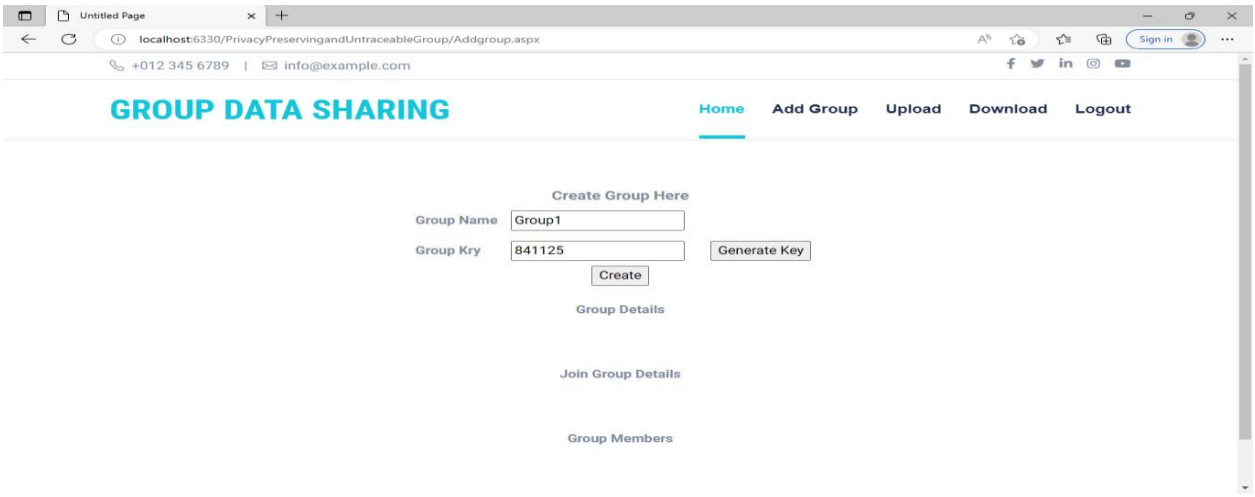

Fig 6.3: Group Creation Page

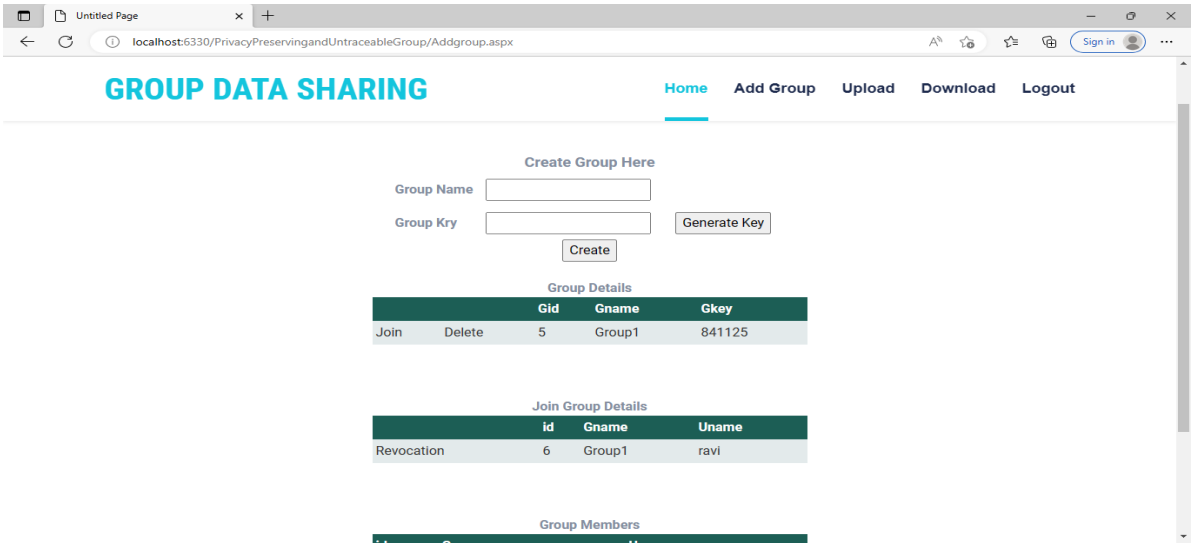

Fig 6.4: Group Details Page

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

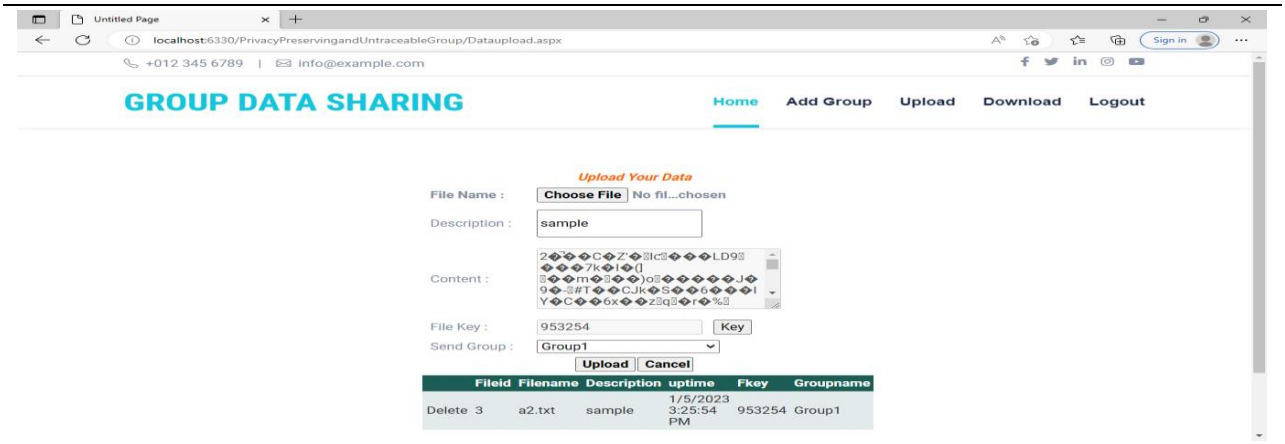

Fig 6.5: File Sharing in the Group

V. CONCLUSION

In this paper, 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.

VI. 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, pp. 59–76.

[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, pp. 1–9.

[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.