International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.027 ISSN: 2581-4621

Secure and Efficient Anonymous Group Data Sharing by SBIBD Technique in Cloud Environment

Mallika P[1],Indhurekha S[2], Jarlin Jeincy[3]
[1]*Assistant Professor, Computer Science and Engineering, Jai Shriram Engineering College, Tiruppur, Tamilnadu*
[2]*Assistant Professor, Computer Science and Engineering, Jai Shriram Engineering College, Tiruppur, Tamilnadu*
[3]*Lecturer, Computer Science and Engineering, Jai Shriram Engineering College, Tiruppur, Tamilnadu*
Corresponding Author Orcid ID : 0000-0001-7606-7576

ABSTRACT
In recent decades, group data sharing in cloud systems has been a prominent issue. With the rise in popularity of cloud computing, achieving safe and efficient data exchange in cloud settings is a pressing issue that must be addressed. Furthermore, achieving both anonymity and traceability in the cloud for data exchange is a difficulty. This work focuses on providing anonymous data exchange and storage in the cloud for the same group with good security and efficiency. A unique traceable group data sharing strategy is developed to allow anonymous multiple users in public clouds by leveraging the key agreement and the group signature. On the one hand, group members can communicate anonymously with regard to the group signature, and on the other hand, group members can track the anonymous members, chat within the group, store and share for secure instant access and updates.
Keywords – Anonymous, Traceability, AES, SBIBD- symmetric balanced incomplete block design, Registration, Secure, Data sharing, Group, Public cloud, Key distribution, Confidentiality.

1. INTRODUCTION

Because of its low energy consumption and resource sharing properties, cloud computing has piqued the interest of most academics when compared to traditionalinformation sharing and communication technologies. Cloud computing may give customers not just seemingly endless computational capabilities, but also seemingly limitless storage resources. One of the mostsignificant services in cloud computing is cloud storage, which allows various sorts of electronic devices to be connected. Furthermore, many types of data information, such as social networks, video editing, and home networks, can freely flow with regard to the cloud storage service. However, group data sharing in the cloud, which refers to a circumstance in which numerous users desire to share information in a group for cooperative reasons, has received little attention. Electronichealth networks, wireless body area networks, and electronic literature in libraries are just a few examples of where group data sharing maybe useful.

In cloud storage, there are two options for sharing data. The first is a one-to- many patterns, which refers to the scenario where one client authorizes access to his/her data for many clients. The second is a many-to-many pattern, which refers to a situation inwhich many clients in the same group authorize access to their data for many clientsat the same time. There are main contributions address challenges for group data sharing in cloud computing elegantly. Therefore, 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 using the SBIBD technique. In the many-to-many group data sharing pattern, it is essential to provideauthentication services to resist misbehaving users. For instance, a misbehaving user may deliberately upload faulty data or misleading data to disturb and influence the cloud storage system. In addition, to resist the different key attack, a fault-tolerant property should be supported in the scheme.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.027 ISSN: 2581-4621

2. PROBLEM STATEMENT

The first is a one-to-many pattern, which describes a situation in which one client grants access to his or her data to several clients. The second pattern is a many-to-many pattern, which describes a situation in which several customers in the same group grant access to their data to multiple clients at the same time. Consider the following scenario in real life: Each member of a study group at a scientific research facility wants to discuss their findings and findings with their colleagues. Members of the same team can access all of the team's results (e.g., new ideas, research findings, and experimental data) in this situation. The upkeep and problems posed by local storage, on the other hand, enhance thedifficulty and workload of group information exchange. Outsourcing data or time-consuming computing activities to the cloud eliminates the upkeep and hassles of local storage while also reducing data redundancy, easing the strain on businesses, academic organizations, and even people. Outsourced data, on the other hand, are vulnerable to beingleaked and tampered with due to the cloud's instability. In many circumstances, consumers have little control over cloud services and cannot ensure the security of data kept there. Furthermore, in some circumstances, the user might wish to share data in the cloud anonymously.

3. EXISTING SYSTEM

In previous studies, Cloud computing storage stores data without a managed access for multiple users in the existing period which decreases the resource and data utilization. No common storage can be used for storing all thefiles because it can be viewed or extracted by all the users. Information security is at high risk. There is no chance of revoking the file access permission given to the user without a dedicated system with keys.

4. THE PROPOSED SYSTEM

The presented scheme can be applied to group data sharing in cloud computing with high security and efficiency. Our scheme is divided in 3 parts: Encryption and decryption, Key generation, file access. The proposed system is that the manager or the group members can share the file in the group. But if the group members want to share the file then they must be registered as a manager first and then they can upload the file. In addition we can create the group on the spot means we have all the list of the members who are registered in the system as members then we select the group members at the time of uploading the file. Also if the manager wants to delete the uploaded

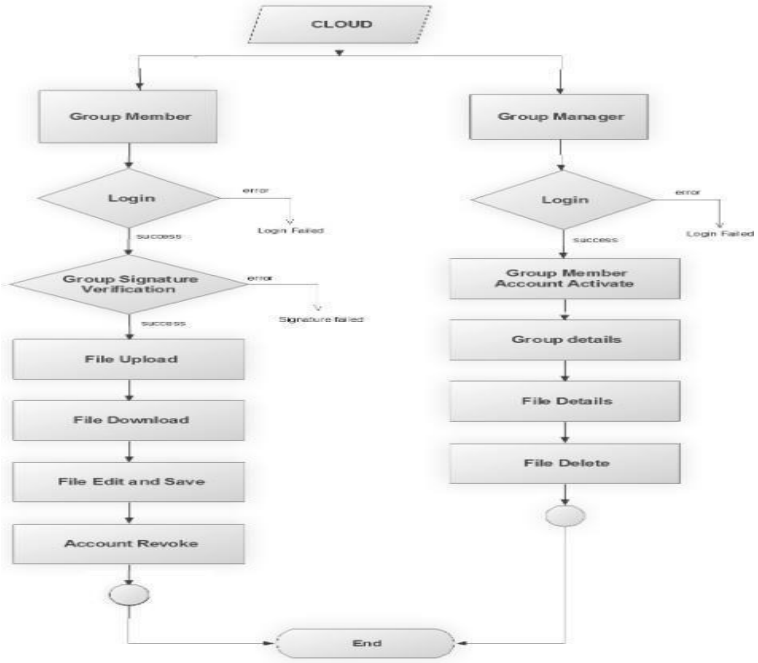

Fig.1 FLOW DIAGRAM

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.027 ISSN: 2581-4621

file then he must ask or take the permission of the group members. Vice versa if the group member wants to delete the file then they will take permission from the manager.

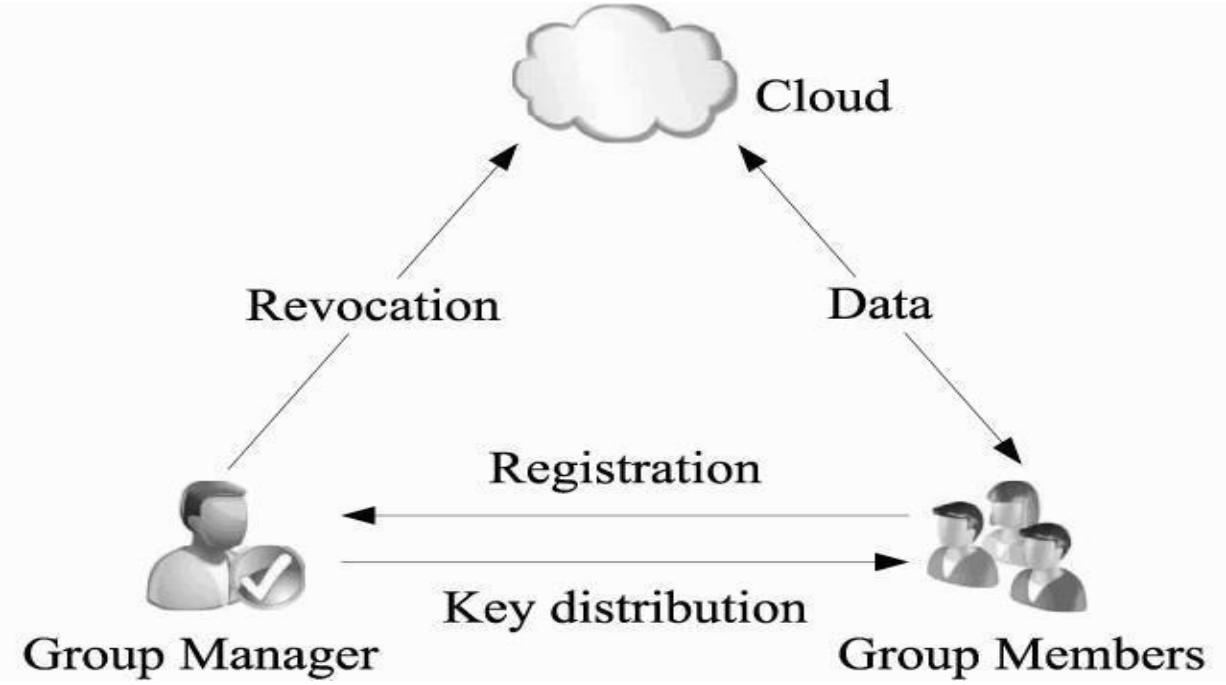

Fig 2. BLOCK DIAGRAM

5. SYSTEM MODELS

5.1 MEMBER MODULE

Based on the SBIBD communication paradigm, the Members module is made up of a succession of users. Members in our system are people. Who share similar interests (for example, bidders, physicians, and businesses) who wish to share data in the cloud. The most concerning issue when users store data on a cloud server is the outsourced data's confidentiality. Users in the same group perform a critical agreement in our system.

5.2 CLOUD MODULE

The cloud appears to give customers practically limitless storage space. In addition to providing users with efficient and easy storage, the cloud may also facilitate data exchange. The cloud, on the other hand, has the trait of being truthful while also being interested. In other words, the cloud will not destroy or change user-uploaded data on purpose, but it will be inquisitive to learn about the data's contents and the user's identity. In our concept, the cloud is a semi-trusted party.

5.3 GROUP ADMIN MODULE

The group manager is in charge of creating system settings, managing group members (i.e., uploading members' encrypted data, approving group members, and exposing a member's true identity), and detecting fault tolerance. In our concept, the group manager is a completely trusted third party for both the cloud and the group members. To begin, people that share a common interest must register with the group manager in order to exchange data in the cloud. In addition, the group manager is in charge of user revocation.

Second, based on the SBIBD structure, all members of the group collaboratively negotiate a shared session key, which may be used to encrypt or decrypt the outsourced data. Finally, if a disagreement arises, the group manager is able to expose the group member's true identity. Note that in our system approach, the group manager's shared conference key handles data uploading and access management, and the encrypted data is kept to a minimum.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 1 Volume No.7 January - February – 2023
DOI:10.46647/ijetms.2023.v07i01.027 ISSN: 2581-4621

6. RESULTS ANDSCREENSHORTS

Fig 3.Home Page

Fig 4. Member Request

7. SYSTEM REQUIREMENTS

a. HARDWARE REQUIREMENTS

SYSTEM : Intel DualCore
HARD DISK : 256 GB
RAM : 2GB

b. SOFTWARE REQUIREMENTS

OPERATING SYSTEM : Windows 10/ Linux
PLATFORM : PYTHON
BACK END : SQL Server
FRONT END : PYTHON

c. TOOLS

CODE IDE : VISUAL STUDIO CODE,NET BEANS

DOI:10.46647/ijetms.2023.v07i01.027 ISSN: 2581-4621

8. FUTURE SCOPE

Further this system to solving the reliability and scalability issues. We can provide the backup group manager. Providing better authentication and allow group access to shared accounts. Extending the web application to support multiplatform OS.

CONCLUSION

We proposed a secure and fault- tolerant key agreement for group data sharing in a cloud storage system in this project. The suggested solution, which is based on the SBIBD and group signature technique, can effectively produce a shared conference key, which can be utilized to safeguard the security of outsourced data while also supporting secure group data sharing in the cloud. This work includes techniques for constructing the SBIBD as well as mathematical explanations of the SBIBD. Furthermore, the group signature approach allows for efficient access control and authentication services. Furthermore, in an anonymous environment, our approach can allow the tracing of user identification.

References

1. Jian Shen; Huijie Yang; P Vijayakumar; Neeraj Kumar "A Privacy - Preserving and Untraceable Group Data Sharing Scheme in Cloud Computing," IEEE Transactions on Dependable and Secure Computing ,Jan 2021.
2. Q. Huang, Y. Yang, W. Yue and Y. He, "Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1607-1618, 1 Oct.-Dec. 2021.
3. J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Comput. Secur.,vol. 72, pp. 1–12, Jan. 2018.
4. T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Trans. Comput., vol. 65, no. 8, pp. 2363–2373, Aug. 2016.
5. J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," Pervasive Mobile Comput., vol. 41, pp. 219– 230, Oct. 2017, doi: 10.1016/j.pmcj.2017.03.013.
6. J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167– 1179, Jun. 2015.
7. X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Trans. Depends. Sec. Comput.,vol. 12, no. 5, pp.546–556, Sep. 2015.
8. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Trans. Parallel Distrib.Syst., vol. 25,no. 9, pp. 2386–2396, Sep. 2014.
9. J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Comput. Secur.,vol. 72, pp. 1– 12, Jan.2018, doi: 10.1016/j.cose.2017.08.007.
10. X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182– 1191, Jun. 2013.
11. Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inf. Sci., vol. 258, pp. 355–370, Feb. 2014.
12. J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," IEEE Trans.Depends. Sec. Comput., to be published, doi: 10.1109/TDSC.2017.2725953.