Secure Data Sharing In Distributed Systems Using Identity Based Encryption

[1]Renuga S, [2]Lavanya K, [3]Mrs.P.Sabeena Burvin, [4]Dr.J.Hemalatha, [5]Mr.C.Pravin Kumar
[1,2] UG Student, Department of Computer Science and Engineering, AAA College of Engg & Tech, Amathur, Sivakasi
[3]Assistant Professor,Department of Computer Science and Engineering,AAA College of Engg & Tech, Amathur, Sivakasi
[4]Professor &Head, Department of Computer Science and Engineering, AAA College of Engg & Tech, Amathur, Sivakasi
[5]Assistant Professor,Department of Computer Science and Engineering,AAA College of Engg &Tech, Amathur, Sivakasi

Abstract: **Effective access control and revocation procedures are necessary for secure data sharing in cloud environments in order to safeguard private data. Using Revocable Storage Identity-Based Encryption (RS-IBE), this project suggests a safe framework for data sharing that guarantees user revocation, dynamic access control, and confidentiality. Four main components make up the system: the Data Provider, who forms a group and invites participants to share files; the Admin, who oversees system functions; the Key Generator, who generates and distributes file decryption keys; and the Data Users, who gain access to shared information. The Key Generator safely distributes the encryption key to authorized users upon file submission. To ensure that the revoked user can no longer access the data, the system immediately revokes access if a member is removed by the Data Provider. It does this by creating a new file key and distributing it exclusively to the remaining group members. This method guarantees smooth and safe data sharing in cloud storage environments, improves data confidentiality, and stops unwanted access. This method guarantees that sensitive files stay safe and does away with the necessity for complete re-encryption. The suggested approach is the perfect answer for safe and scalable cloud-based data sharing since it combines effective key management, access control systems, and dynamic user revocation. The solution is ideal for businesses that need to share data in a regulated and private manner since it improves data security, stops unwanted access, and lowers computational overhead.**

Key words: **Access control, Batch auditing, Cloud computing security, Cloud storage, Cryptographic verification, Data integrity, Data modification tracking, Data sharing, Digital signatures, Efficiency in cloud services, Proxy re-signatures, Public auditing, Shared data security, Third-party auditing, User revocation.**

I. INTRODUCTION

Secure data sharing in cloud environments is essential in today's digital age to prevent unwanted access to sensitive data while maintaining effective access control. Conventional encryption methods are ineffective for dynamic group-based data sharing because they frequently have issues with key management, scalability, and user revocation. This project introduces a secure data-sharing system employing Revocable Storage Identity-Based Encryption (RS-IBE), which provides a robust mechanism for access control, secrecy, and dynamic user revocation. Four essential components make up the system: the Data Provider, which forms groups and distributes encrypted information; the Admin, who oversees system functions; the Key Generator, which provides decryption keys; and the Data Users, who safely access shared files. The Key Generator makes sure that the decryption key is only given to authorized users when a file is shared. In order to avoid unwanted access by the removed user, the system securely distributes the file key to the other members only after a member is revoked. This method improves data security, scalability, and flexibility by incorporating user revocation and efficient key management, which makes it a good choice for safe cloud-based data sharing.

Cloud-based data storage and sharing services (like Dropbox and Google Drive) make it simple for users to collaborate in groups by exchanging data. More precisely, after a user produces shared data in the cloud, all group members can view and edit the shared data as well as distribute the most recent

version to the other group members. Despite cloud providers' assurances of a more secure and dependable environment, human error and hardware/software malfunctions can still jeopardize the security of data stored in the cloud.Many methods have been put forth to safeguard the integrity of data stored in the cloud. Each data block in these systems has a signature attached to it, and the accuracy of each signature is necessary for the data to remain intact.

The ability for a public verifier to effectively verify data integrity in the cloud without downloading the complete data—known as public auditing—is one of the most important and prevalent characteristics of these techniques. This public verifier could be a third-party auditor (TPA) that can offer customers data integrity verification services or a client who wants to access cloud data for specific reasons (such as search, computing, data mining, etc.).The majority of earlier research focuses on auditing the accuracy of personal data. In contrast to these research, a number of recent studies concentrate on protecting identify privacy from public verifiers when examining the accuracy of shared data. Regretfully, while auditing the accuracy of shared data in the cloud, none of the aforementioned procedures take user revocation efficiency into account.

When a user makes changes to a block in shared data, she must also calculate a new signature for the updated block. various blocks are signed by various users as a result of user modifications. When a user leaves the group or behaves inappropriately, they must be removed from the group for security reasons. This should prevent the revoked user from accessing and changing shared data, and the group will no longer be able to use the signatures created by this revoked user.The blocks that were previously signed by the revoked user must therefore be re-signed by an existing user in the group, even though the content of shared data remains unchanged after user revocation. Therefore, only the public keys of current users may be used to confirm the integrity of all the data.

II. METHODOLOGY

Existing Methodology:

The current system uploads files to the server without requiring the user to sign them each time. Since there is no direct method to confirm that the data is unchanged, the absence of user signatures makes it challenging to guarantee the integrity of shared data. In collaborative settings, there may be security problems if there is no way to confirm authenticity since illegal changes or tampering with the data could go unnoticed.

Data security is further complicated by the fact that the server is not part of the same trusted domain as the group's users. Because the server is an external entity, using it to handle data without taking extra security precautions leaves the shared data vulnerable to potential risks like malicious alteration, unauthorized access, and data corruption. Since users are unable to confirm that the stored data is still consistent with the version that was initially submitted, data integrity cannot be completely guaranteed in such a situation.

Because it creates serious security flaws, outsourcing each user's private key to the server is not a workable approach. Unauthorized parties may obtain users' private keys if the server is compromised, which could result in data breaches, identity theft, and confidentiality loss. To maintain data integrity and safeguard user credentials from potential attacks, a more secure method is needed. Putting in place a strong verification method, like proxy re-signatures or cryptographic signatures, can help allay these security worries and boost confidence in cloud-based data-sharing platforms.

Proposed Methodology:

In order to guarantee secrecy, controlled access, and dynamic user revocation in cloud storage environments, the suggested methodology focuses on safe and effectivedata sharing utilizing Revocable Storage Identity-Based Encryption (RS-IBE). The Data Provider, Admin, Key Generator, and Data Users are the four primary components of the system. Group creation, member addition and removal, and encrypted file sharing are all handled by the data provider. Identity-Based Encryption (IBE), in which the encryption key is created based on the recipient's identity or characteristics, is used to encrypt files when they are uploaded. Authorized Data Users can safely access shared files by using the decryption keys that the Key Generator provides.

The system automatically generates a new encryption key and securely distributes it solely to the remaining group members in order to handle user revocation

when a member is removed. This assures that the revoked user can no longer access previously shared files, preventing unwanted data access. This technique dynamically updates keys without changing stored data, lowering computational overhead and increasing efficiency in contrast to typical encryption techniques that necessitate re-encrypting all files upon user withdrawal. In order to track user activity, identify unwanted access attempts, and guarantee adherence to security regulations, the system also integrates logging and security monitoring.

A scalable, adaptable, and extremely secure data-sharing framework for cloud storage settings is offered by the suggested technique, which combines safe identity-based encryption, dynamic revocation, and effective key management

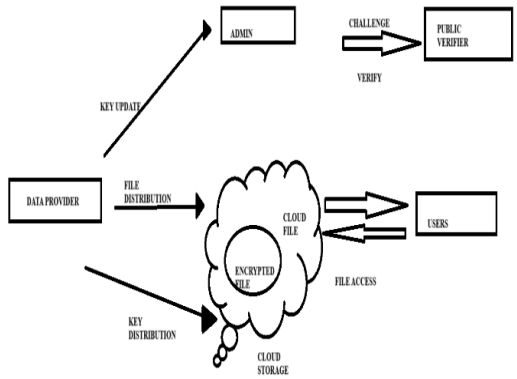


Figure 1: proposed system architecture

III. RESULTS AND DISCUSSION

1. User Management Module

Within the system, role assignments, access control, and user authentication are handled by the User Management Module. Each of the four main roles—Data Provider, Admin, Key Generator, and Data Users—is defined, and each has particular rights. Group creation, member additions and deletions, and file access management fall under the purview of the Data Provider. The administrator keeps an eye on security regulations, manages system operations, and guarantees seamless functioning. The Key Generator is a reliable source that safely creates and provides authorized users with encryption and decryption keys. Shared files are sent to data users, who can only access them with a working decryption key.To guarantee that only authorized users can access particular capabilities, the system employs robust authentication procedures. Additionally, it keeps a thorough record of user actions, guaranteeing security and accountability in the data-sharing setting. This module is essential for protecting sensitive data and stopping unwanted access since it enforces stringent role-based access control.

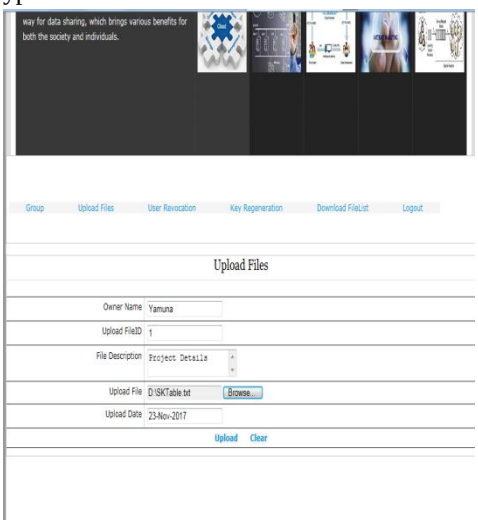
2. Group Management Module

Structured access control for shared files is ensured by the Group Management Module, which makes it easier to create and manage user groups securely. The Data Provider can add users who need access to shared files and form groups according to project requirements or security levels. Only authorized members can access encrypted data in each group, which functions as an isolated environment. The module also includes functionality for adding new members, updating group settings, and managing permissions. A user's access to a group is immediately ended upon revocation, guaranteeing that they are unable to read files or obtain encryption keys.When a user is removed, the system dynamically updates the encryption keys and only redistributes them to the remaining members in order to maintain security. This keeps revoked users from abusing previously granted permissions and guarantees that sensitive data is protected. The module enforces stringent security controls to stop unwanted file access while facilitating smooth cooperation.

3. File Encryption and Upload Module

Before data is saved on the server, the File Encryption and Upload Module guarantees its integrity and confidentiality. Identity-Based Encryption (IBE), a cryptographic technology that secures data by linking encryption keys with user identities, is applied to files uploaded by data providers. This eliminates the need for traditional key distribution methods and assures that only authorized users can decrypt the file. The file is safely saved on the cloud after it has been encrypted, guarding against breaches and unwanted access.To guarantee that files are only accessible by specified user groups, this module also incorporates access control measures. Even if an attacker manages to access cloud storage, they will be unable to obtain relevant data without the decryption key because

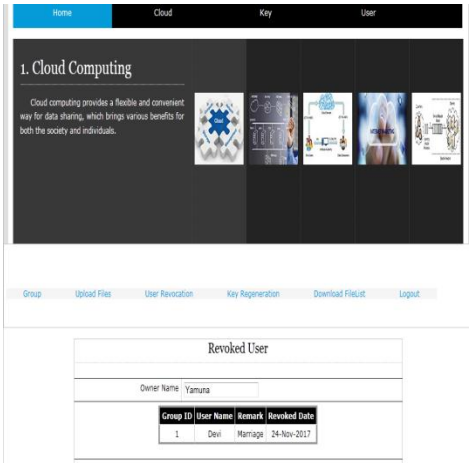
encryption takes place prior to data storage. This module ensures end-to-end security and removes the possibility of data disclosure from compromised cloud infrastructure by utilizing IBE-based encryption.



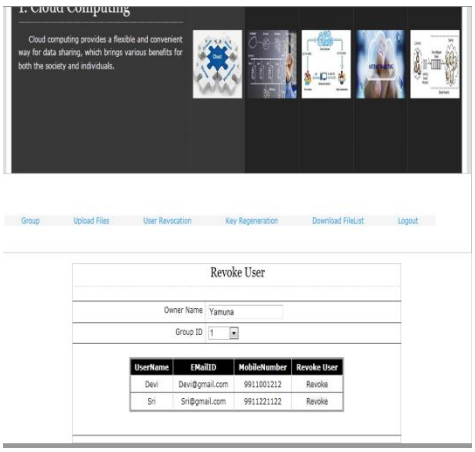
Screenshot 1: File Upload

4. Key Distribution and Revocation Module

In order to maintain secure file access control, the Key Distribution and Revocation Module is essential for maintaining encryption and decryption keys. The Key Generator is in charge of safely allocating decryption keys to approved Data Users in accordance with their group membership and identification. A special decryption key is given to each user who joins a group, allowing them to view encrypted files. But when a user is deleted, the system initiates an automatic revocation procedure that regenerates the shared file's encryption key.Only the remaining group members are securely given access to this new file key, guaranteeing that the revoked user will never again be able to access it. This module improves the process by dynamically updating the keys without harming stored data, in contrast to standard encryption systems that necessitate re-encrypting all files upon user revocation. This lowers computational overhead, increases efficiency, and guards against illegal access to previously shared files. Revocable identity-based encryption is integrated into this module to provide strong security in dynamic data-sharing settings.



Screenshot 2: Revoke User



Screenshot 3: Reupload

5. File Access and Download Module

Only authorized users are able to access and decrypt shared files thanks to the File Access and Download Module. Before allowing access, the system confirms the identity and group membership of the Data User. The most recent decryption key is sent to the user by the Key Generator if they are still a member of the group, enabling them to safely decrypt and download the file. When a user's access is revoked, the system stops them from downloading files or getting fresh decryption keys. Secure transmission protocols are also enforced by this module to guard against data interception during downloads.To further ensure security and transparency, access logs are kept to monitor every file retrieval activity. This module keeps critical information safe and prevents data breaches by limiting access to authorized users only, even when users join or leave groups on the fly.

V. CONCLUSION

In cloud-based settings, the suggested solution for safe data sharing on a server that makes use of Revocable Storage Identity-Based Encryption (RS-IBE) guarantees effective user revocation, access control, and a high degree of security. Files are safely protected before to storage by utilizing IBE-based encryption, which restricts access to them to authorized users who possess the decryption keys provided by the Key Generator.The data provider can add or delete users from user groups thanks to the system's dynamic management, which also makes sure that revoked users can't access shared files. This technique creates a new encryption key and only redistributes it to active members, greatly increasing computational efficiency and lowering overhead in contrast to conventional encryption techniques that necessitate full re-encryption upon user revocation.

By linking encryption keys to user identities or characteristics, the system also guarantees fine-grained access control, avoiding data breaches and unwanted access. By watching user interactions, identifying questionable conduct, and averting any dangers, the combination of activity logging and security monitoring improves protection even further. For businesses, organizations, and collaborative cloud platforms where user management, data confidentiality, and integrity are crucial, this methodology is especially advantageous. All things considered, the suggested RS-IBE-based method offers a scalable, safe, and effective way to share data in cloud environments. It is the perfect framework for real-world applications needing privacy-preserving and restricted access procedures because it successfully strikes a balance between data security, key management, and dynamic user revocation.

For data exchange in cloud contexts, the suggested Revocable Storage Identity-Based Encryption (RS-IBE) solution offers a safe and effective architecture. Its functionality, scalability, and security can be further improved with a few additions, though. Combining artificial intelligence (AI) and machine learning (ML) for automated threat and anomaly detection is one possible improvement. This can assist in real-time identification of suspicious activity, unauthorized access attempts, and possible security breaches. Furthermore, by removing single points of failure and guaranteeing tamper-proof key distribution, the use of Blockchain technology for decentralized key management might improve security even more. Fine-grained access control with Attribute-Based Encryption (ABE), which permits more adaptable access permissions based on user roles, departments, or access levels, is another area that needs development.

For large enterprises with intricate access control needs, this would offer improved security. Additionally, using lightweight cryptographic techniques to optimize the key revocation process can lower computational overhead and increase system efficiency in resource-constrained situations like mobile and Internet of Things devices. Last but not least, expanding the system to accommodate several cloud storage platforms can enhance data availability and redundancy, guaranteeing safe and easy access to shared files from various cloud service providers. The suggested system can develop into a more intelligent, scalable, and resilient cloud-based secure data-sharing solution that is appropriate for a variety of real-world applications by incorporating these improvements.

REFERENCES

[1] Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: An enterprise perspective on risks and compliance. O'Reilly Media.

[2] David, S. (2011). Securely storing (encrypting) data in an ASP.NET application. Retrieved from https://stackoverflow.com/questions/7745385/securely-storing-encrypting-data-in-an-asp-net-application

[3] Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. International Journal of Distributed Sensor Networks, 8(2), 1-12.

[4] Rong, C., Nguyen, H., & Jaatun, M. G. (2014). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 40(6), 1806-1827.

[5] Kshetri, N. (2014). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 38(9), 1-13.

[6] Li, X., Li, M., & Li, J. (2015). Secure and efficient data sharing in cloud computing. IEEE

Transactions on Knowledge and Data Engineering, 27(2), 442-455.

[7] Liu, X., Liu, J., Guo, S., & Wang, Q. (2015). Towards secure cloud storage via dynamic virtual file allocation and verification. Journal of Network and Computer Applications, 49, 41-52.

[8] Ahmad, I., Naseer, M., & Javaid, N. (2017). A survey on secure data sharing in cloud computing. Journal of Network and Computer Applications, 79, 185-200.

[9] Al-Rimy, B. A., & Al-Zobbi, M. M. (2018). The security of cloud computing. In S. Jabbar, J. Qadir, & Y. Zaki (Eds.), Handbook of Research on Cloud Computing and Big Data Applications in IoT (pp. 22-39). IGI Global.

[10] Binzagr, A., & Soh, B. (2018). Secure data sharing in cloud computing: A systematic literature review. International Journal of Cloud Computing, 7(3), 278-298.

[11] Sattar, S., Alhaisoni, M., & Gharibi, W. (2018). Enhancing security in cloud storage using hybrid cryptography. Future Generation Computer Systems, 87, 693-703.

[12] Sivanandam, S. N., & Kannan, A. (2018). A secure data sharing framework for cloud computing. Journal of Ambient Intelligence and Humanized Computing, 9(5), 1675-1688.

[13] Alshehri, M., & Aldossary, M. (2019). Secure data sharing in cloud computing: Challenges and solutions. Journal of Network and Computer Applications, 138, 85-97.

[14] Chen, J., Zhao, X., Chen, J., & Wu, J. (2019). A secure data sharing scheme for cloud computing based on ciphertext-policy attribute-based encryption. IEEE Access, 7, 102535-102546.

[15] Seelam, S., Bhattacharjee, S., & Sahoo, B. K. (2019). Enabling secure and efficient data sharing in cloud computing. Journal of Ambient Intelligence and Humanized Computing, 10(7), 2719-2732.

[16] Sharma, A., Dutta, A., & Deka, G. C. (2019). Secure data sharing in cloud computing: A systematic review and future directions. Journal of Ambient Intelligence and Humanized Computing, 10(7), 2631-2653

[17] Islam, M. M., Kulkarni, M. A., & Sohrabi, B. (2019). A secure data sharing framework for collaborative edge and cloud computing. Future Generation Computer Systems, 92, 61-70.

[18] Aeri, M. (2020). Secure data sharing in cloud computing systems: Techniques and applications. Turkish Journal of Computer and Mathematics Education, 11(3), 2087-2094.

[19] Zhang, L., & Chen, Y. (2023). Secure Group Data Sharing Using Revocable Identity-Based Encryption in Cloud Environments. IEEE Transactions on Cloud Computing, 11(2), 315-326.

[20] Li, M., Wu, H., & Zhou, J. (2023). Fine-Grained Access Control for Cloud Storage Using Improved Identity-Based Encryption. Future Generation Computer Systems, 144, 36-49.

[21] Wang, X., & Li, F. (2023). Secure Data Collaboration in Cloud Using Threshold Identity-Based Encryption. Journal of Cloud Security, 10(3), 142–157.

[22] Yadav, R., & Mehta, P. (2024). Hierarchical Identity-Based Encryption for Multi-Level Cloud Data Sharing. Information Sciences, 648, 115–132.

[23] Kumar, R., & Patel, S. (2024). Efficient and Privacy-Preserving Data Sharing in Cloud Using Identity-Based Proxy Re-encryption. Journal of Network and Computer Applications, 215, 103497.

[24] Patel, H., & Iqbal, M. (2024). Group Sharing with Time-Controlled Identity-Based Encryption in Cloud Environments. Journal of Systems and Software, 205, 111481.

[25] Nguyen, T. H., & Zhao, Q. (2024). Revocable and Scalable Group Data Sharing Based on IBE in Public Clouds. Journal of Cloud Computing: Advances, Systems and Applications, 13(1), 57.