International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 1 Jan. 2026, pp: 143-150 www.ijaem.net ISSN: 2395-5252

Fine Grained Two Factor Authentication with Data Sharing in Cloud Storage

[1]Dr. K.E.Kannammal, [2] Dr. Y.BabyKalpana, [3]Ms. N.Lavanya
[1]*Professor &Head of the Department,* [2]*Professor,* [3]*Student*
[1,2,3]*Department of Computer Science and Technology,*
[1,2,3]*Sri Shakthi Institute of Engineering and Technology, Coimbatore, India*

Date of Submission: 02-01-2026 Date of Acceptance: 10-01-2026

ABSTRACT

In the digital age, cloud storage has emerged as a cornerstone of data management, offering unparalleled flexibility and efficiency for storing and sharing data. The convenience and scalability of cloud services have enabled users and organizations to access and disseminate information from anywhere, at any time, fostering collaboration and innovation across the globe. However, this ease of access also introduces significant security vulnerabilities, particularly concerning the confidentiality and integrity of sensitive information shared via the cloud. The protection of sensitive data in cloud environments poses complex challenges, primarily due to the persistent threats of unauthorized access and data breaches. Traditional cryptographic methods have served as the bedrock for securing data in transit and at rest. Yet, these approaches often fall short in addressing the dynamic and multifaceted nature of data sharing in cloud storage, where the granularity of access and the flexibility of data sharing permissions are paramount. Amid these challenges, the mechanism of key management emerges as a critical concern. The traditional single-layered encryption key systems, while providing a baseline for security, are not infallible. The singular point of failure in such systems—a compromised key—can lead to unauthorized data exposure. Furthermore, the static nature of these keys does not align well with the dynamic requirements of cloud-based data sharing, where user attributes and permissions may frequently change.

Recognizing these limitations, our project introduces a novel "Fine-Grained Two-Factor Protection Mechanism for Data Sharing in Cloud Storage," aimed at enhancing the security and flexibility of cloud storage services.

KEYWORDS: Data sharing in cloud storage, enhancing security, encryption key systems.

I. INTRODUCTION

Data sharing in cloud storage is receiving substantial attention in Information Communications Technology, since it can provide users with efficient and effective storage services. To protect the confidentiality of the shared sensitive data, the cryptographic techniques are usually applied. However, the data protection is still posing significant challenges in cloud storage for data sharing. Among them, how to protect and revoke the cryptographic key is the fundamental challenge. To tackle this, we propose a new data protection mechanism for cloud storage, which holds the following properties.

1) The cryptographic key is protected by the two factors. Only if one of the two factors works, the secrecy of the cryptographic key is held.
2) The cryptographic key can be revoked efficiently by integrating the proxy re-encryption and key separation techniques.
3) The data is protected in a fine-grained way by adopting the attribute based encryption technique. Furthermore, the security analysis and performance evaluation show that our proposal is secure and efficient, respectively.

II. LITERATURE SURVEY

Here, we provide a brief overview of cryptographic systems that have comparable features required in the data sharing scenario and discuss why they fall short of our objectives. 2.1 Cryptographic solutions for the problem of key exposure:To address the issue of private key exposuresuggested a key-insulated public key system. There are two keys in this kind of system. One, known as the master secret key, is kept in a security device, which is a physically safe but computationally constrained device; the other, known as the master secret key, is kept in an insecure device, such as a computer, and can be updated on a regular basis. Both the public key and the master secret key are always the same. Still, the further and more frequently the private key notifications, the more chance of master secret key

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 1 Jan. 2026, pp: 143-150 www.ijaem.net ISSN: 2395-5252

exposes. Hanaoka et al. developed parallel key isolated public key encryption in 2006 as a solution to this issue. Two separate master secret keys are used in subsequent studies, which greatly lowers the possibility of master secret key exposure. However, in the random oracle model, the security proof is obtained. A parallel key isolated public key encryption secure in the conventional paradigm was proposed by Libert et al. in 2007. The authors of Liu et al. used the key insulated methods in 2008 to address the ring signature key exposure issue. The security device is used to periodically update each user's private key in all of the aforementioned systems. Furthermore, the security device does not participate in the decryption process after the private key has been updated. However, the criteria in the cloud computing data sharing scenario state that the security device must be involved in every stage of decryption and that the user's private key should not be updated continuously.

III. EXISTING SYSTEM

In the existing system, users are able to upload files to a server through a web interface. However, the system lacks any form of encryption or secure storage for these files. Uploaded files remain in their original, unencrypted state on the server, which poses potential security risks. Users can access and download their files directly from the server without any encryption or decryption processes in place, leaving sensitive data vulnerable.

3.1 DISADVANTAGES OF EXISITING SYSTEM

- Lack of data security, leaving files vulnerable to breaches.
- Limited data protection relying solely on server-side security.
- Risk of data exposure due to plain, unencrypted storage.
- Absence of secure access controls, posing unauthorized access risks.

IV. PROPOSED SYSTEM

The proposed system represents a substantial improvement in terms of security and data protection. Users can still upload files via the web interface, but administrators are now responsible for enhancing security. When a user uploads a file, administrators are promptly notified. They employ robust encryption techniques, along with securely managed encryption keys to encrypt the files before storage. Encrypted files are temporarily safeguarded on the server, ensuring that even if the server's security is compromised, the files remain protected. Additionally, the system integrates with cloud storage services, allowing administrators to securely upload encrypted files, thus enhancing data availability and durability. When users require access to their files, administrators retrieve the encrypted files from cloud storage, decrypt them using the encryption keys, and then provide secure access to the decrypted content. With stringent security measures, including key management, access controls, and encrypted communication, coupled with regular maintenance and updates, this proposed system not only fortifies data security but also guarantees reliability and resilience. Comprehensive documentation is provided for both users and administrators, offering guidance on file management, retrieval, and best practices, making it a comprehensive solution for data protection and accessibility.

4.1 ADVANTAGES OF PROPOSED SYSTEM

- Enhanced data security through robust encryption.
- Secure on-premises storage even in the event of server compromise.
- Integration with cloud storage for improved data availability.
- Controlled access with only authorized personnel managing decryption.
- Comprehensive security measures including key management and access controls.
- Documentation and guidance for secure file management.
- Compliance with data privacy regulations for handling sensitive data.

V. MODULE DESCRIPTION

A module is a Hardware and software component or part of a program that contain one or more routines. One or more independently developed modules make up a program. The project **"Fine-Grained Two-Factor Protection Mechanism for Data Sharing in Cloud Storage"** consists of two main modules they are,

- ✓ User Uploads a File
- ✓ Server Receives and Encrypts the File
- ✓ Secure Storage in the Cloud
- ✓ Providing the File to Users

1. User Uploads a File:

- Create a user-friendly web interface where users can upload files to your server.

2. Server Receives and Encrypts the File:

- When a user uploads a file, your server should receive it.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 1 Jan. 2026, pp: 143-150 www.ijaem.net ISSN: 2395-5252

- The admin, who has access to the server, should be notified of the new upload.
- The admin should then choose to encrypt the file using a secure encryption algorithm and a strong encryption key. The key should be securely managed and protected.
- The encrypted file should be stored securely on the server or temporarily in a designated secure location.

3. Secure Storage in the Cloud:

- Configure a cloud storage service to store the encrypted files.
- The admin should have the necessary credentials and permissions to upload files to the cloud storage.
- When the admin encrypts the file, they should also upload it to the cloud storage. Be sure to secure the communication between your server and the cloud storage service.

4. Providing the File to Users:

- When a user requests a specific file, the admin should be notified.
- The admin should download the encrypted file from the cloud storage.
- Using the encryption key (which should be securely managed and accessible only to the admin), the admin should decrypt the file.
- The decrypted file can then be securely provided to the user for download.

VI. SYSTEM DESIGN

6.1 FILE DESIGN

System design is the process of planning a new system to complement or altogether replace the old system. The purpose of the design phase is the first step in moving from the problem domain to the solution domain. The design of the system is the critical aspect that affects the quality of the software. System design is also called top-level design. The design phase translates the logical aspects of the system into physical aspects of the system.

6.2 INPUT DESIGN

Input design is the process of converting the user-oriented. Input to a computer based format. The goal of the input design is to make the data entry easier, logical and free error. Errors in the input data are controlled by the input design. The quality of the input determines the quality of the system output.

The entire data entry screens are interactive in nature, so that the user can directly enter into data according to the prompted messages. The users are also can directly enter into data according to the prompted messages. The users are also provided with option of selecting an appropriate input from a list of values. This will reduce the number of error, which are otherwise likely to arise if they were to be entered by the user itself.

6.3 OUTPUT DESIGN

Output design is very important concept in the computerized system, without reliable output the user may feel the entire system is unnecessary and avoids using it. The proper output design is important in any system and facilitates effective decision-making. The output design of this system includes various reports.

Computer output is the most important and direct source of information the user. Efficient, intelligible output design should improve the system's relationships with the user and help in decision making. A major form of output is the hardcopy from the printer.

- Admin allocate user id and password to the users.
- Different products displayed to user.
- Shopping Cart generates for users.
- Displays search result.

6.4 DATABASE DESIGN

A database should provide integration, Integrity and a data independence table in a database contains information pertaining to a specific entity. To maintain the tables in an effective way, it should be normalized to ensure that the number of tables does not exceed the optimum level unless it is mandatory. To prevent unauthorized access, security measures have been provided. This may prevent unauthorized persons using data that is private. The normalization techniques have been used to design the table such that the use of all the tables is made easy.

Table 01: User Registration

COLUMN NAME	DATA TYPE	WIDTH	DESCRIPTION
Uname	varchar	20	User name

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 1 Jan. 2026, pp: 143-150 www.ijaem.net ISSN: 2395-5252

Pass	varchar	20	password
Mailid	varchar	20	Mail id
Password	varchar	-	password
Confirm password	varchar	20	Confirm password

Table 02: User Login
Primary Key: user_id

COLUMN NAME	DATA TYPE	WIDTH	DESCRIPTION
login_id	number	10	Login Id
user_name	varchar	20	User name
Pass	varchar	20	Password

Table 03: Upload

COLUMN NAME	DATA TYPE	WIDTH	DESCRIPTION
user_id	varchar	20	User Id
Upload_file	varchar	20	Upload file
Secret_key	varchar	20	Set secret key

Table 04: download

COLUMN NAME	DATATYPE	WIDTH	DESCRIPTION
File_id	varchar	20	Put secret key
File_name	int	20	Uploaded file name
Sec_key	varchar	20	put secret key
d_file	-	-	Download file

International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 1 Jan. 2026, pp: 143-150 www.ijaem.net ISSN: 2395-5252

VII. RESULTS

FIGURE 1: STARTING SERVER

FIGURE 2: HOME PAGE

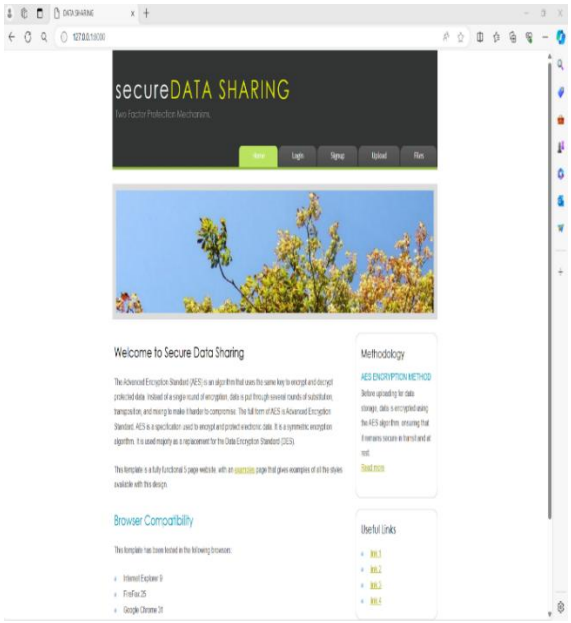
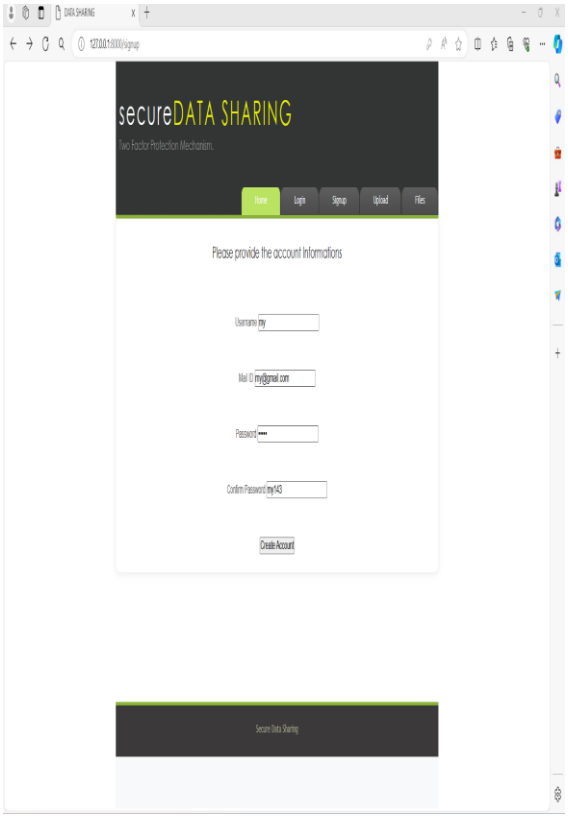


FIGURE 03 : ACCOUNT SIGN UP



International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 1 Jan. 2026, pp: 143-150 www.ijaem.net ISSN: 2395-5252

FIGURE 04: ACCOUNT LOGIN

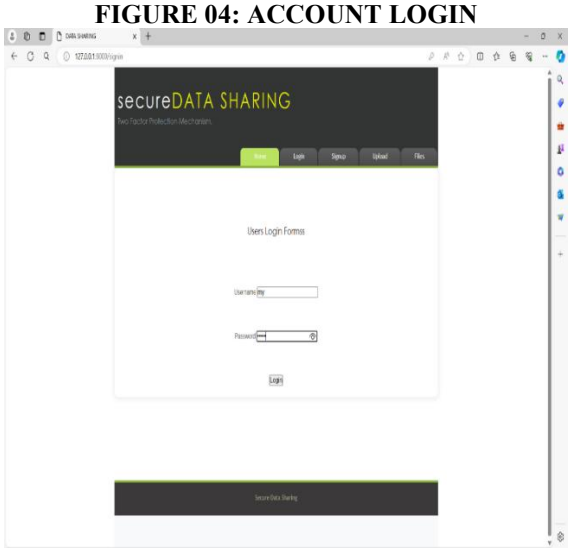


FIGURE 5: UPLOADING FILES

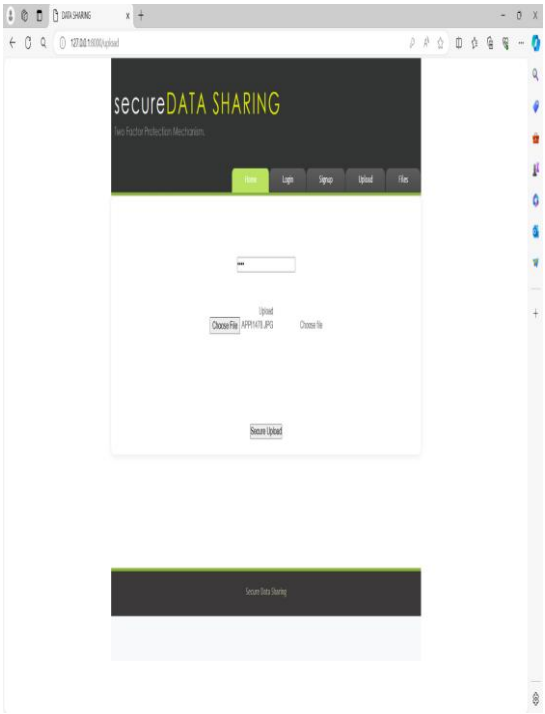
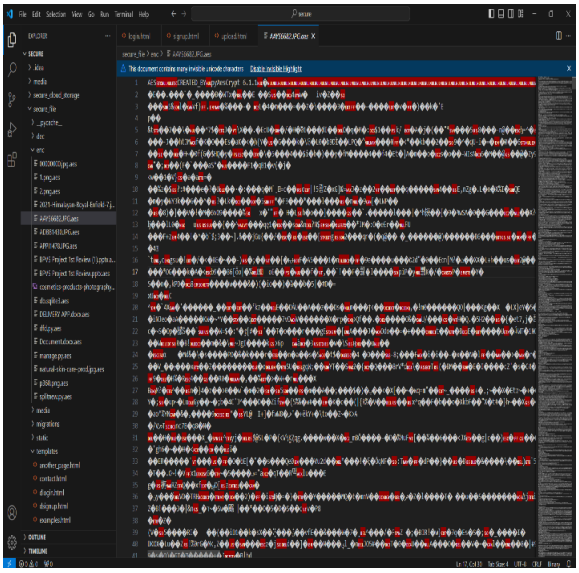


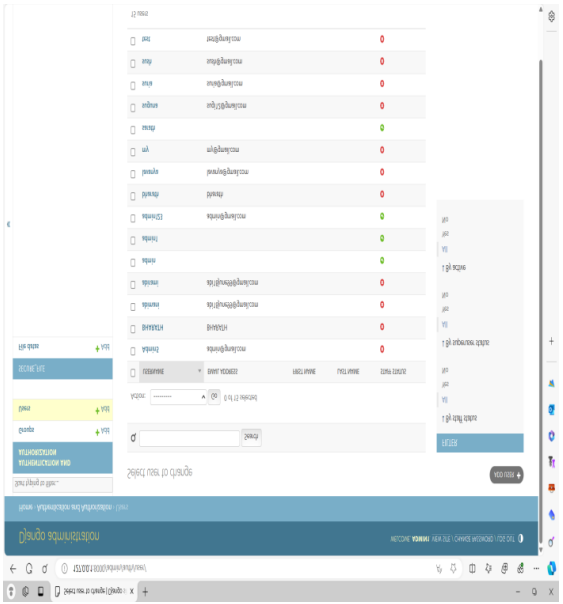
FIGURE 6: VIEWING FILES

FIGURE 7: ADMINISTRATOR VIEW



International Journal of Advances in Engineering and Management (IJAEM)
Volume 8, Issue 1 Jan. 2026, pp: 143-150 www.ijaem.net ISSN: 2395-5252

FIGURE 8: ADMIN MANAGE USER UPLOADED FILES



VIII. CONCLUSION

The advent of cloud computing has undeniably revolutionized the way data is stored, accessed, and shared across the globe, offering unparalleled efficiency and flexibility. However, the concomitant security challenges, particularly concerning the confidentiality and integrity of sensitive data shared in cloud environments, necessitate innovative solutions. Our project, entitled "Fine-Grained Two-Factor Protection Mechanism for Data Sharing," stands as a testament to the potential of advanced cryptographic methods in addressing these pressing concerns.Through the implementation of a dual-factor key protection mechanism, our approach significantly elevates the security threshold, ensuring that the cryptographic keys safeguarding sensitive data are robust against unauthorized access. The integration of proxy re-encryption and key separation techniques streamlines the process of key revocation and reissuance, offering a dynamic solution that is adept at navigating the fluid landscape of cloud storage permissions and user attributes. The security analysis and performance evaluation of our system underscore its efficacy and efficiency. By meticulously addressing the foundational challenge of protecting and revoking cryptographic keys in a cloud storage context, our mechanism not only fortifies the confidentiality of shared data but also introduces a scalable and flexible model for data sharing.

In conclusion, our project contributes a significant step forward in the quest for secure, efficient, and flexible data sharing. By innovatively addressing the critical aspects of key protection, revocation, and access control, we pave the way for more resilient cloud storage systems that can adeptly meet the demands of the digital age. The implications of our work extend beyond the technical realm, offering a blueprint for a future where the secure and seamless sharing of information is not only possible but assured.

8.1 FUTURE ENHANCEMENT

The future of "Fine-Grained Two-Factor Protection Mechanism for Data Sharing in Cloud Storage," our focus will pivot towards embracing emerging technologies, enhancing user experience, and ensuring scalability and interoperability across diverse cloud platforms. Key areas for enhancement include integrating quantum-resistant algorithms and block chain for improved security and transparency, refining encryption schemes to be more adaptive and context-aware, and optimizing the system for performance and environmental sustainability.

Furthermore, developing standardized protocols for cross-platform compatibility and advancing automated threat response mechanisms will be crucial. By addressing these facets, the project aims to remain adaptable and robust, safeguarding against evolving cyber security threats while supporting the ever-growing demands of digital data sharing and cloud storage solutions.

REFERENCES

[1]. J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, “Fine-grained two factor accesscontrol for web-based cloud computing services,” IEEE Transactions on Information Forensicsand Security, vol. 11, no. 3, pp.484–497, 2016.

[2]. C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, “Chosen cipher text secure attribute-basedencryption with outsourced decryption” in Australasian Conference on Information Security andPrivacy. Springer, 2016, pp.495– 6 based storage system in a cloud-of-clouds,” Computers,IEEE Transactions on, vol. 63, no. 1, pp. 31–44, 2014.

[3]. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving publicauditing for secure. cloud storage,” Computers, IEEE Transactions on, vol. 62, no. 2, pp.362–375, 2013.

[4]. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, “Dynamic audit servicesfor outsourced storages in clouds,” Services

Computing, IEEE Transactions on, vol. 6, no. 2, pp.227–238, 2013.

[5]. C., Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storageservices in cloud computing," Services Computing, IEEE Transactions on, vol. 5, no. 2, pp.220–232, 2012.