# A SECURE GROUP DATA SHARING IN CLOUD WITH DATA INTEGRITY

**Dr.S.Subashree M.E.,Phd**
Assistant Professor
Department of Computer Science and Engineering
E.G.S.Pillay Engineering college(Autonomous),
Nagapattinam, India
subashree@egspec.org

**Karthik. S**
Department of Computer Science and Engineering
E.G.S.Pillay Engineering college(Autonomous),
Nagapattinam, India
karthikarthisankar@gmail.com

**Krishnaraj. S**
Department of Computer Science and Engineering
E.G.S.Pillay Engineering College(Autonomous),
Nagapattinam, India
krishnaram1004@gmail.com

**Rameshkanna. S**
Department of Computer Science and Engineering
E.G.S.Pillay Engineering college(Autonomous),
Nagapattinam , India
Kuttyramesh801@gmail.com

## Abstract

*Cloud computing provides high performance, accessibility and low cost for data storing and sharing, provides a better consumption of resources. In cloud computing, cloud service providers compromise an abstraction of infinite storage space for clients to mass data. It can help clients diminish their financial overhead of data managements by drifting the local managements system into cloud servers. However, security concerns develop the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a mutual approach is to encrypt data files before the clients upload the encrypted data into the cloud. Cloud storage services can help clients reduce their monetary and maintenance overhead of data managements. It is complex to design a secure data sharing scheme, especially for dynamic groups in the cloud. To overcome the problem, here propose a secure data sharing scheme for frequently changed groups. In this work, an AES based encryption scheme is proposed which incorporates the cryptographic approaches with Group Data Sharing and also an anonymous control scheme to address the privacy in data as well as the user identity privacy in current access control schemes. If the group member can be revoked means, automatically change public keys of existing group and no need encrypt again the original data. Any user in the group can access data source in the cloud and revoked users does not allowed accessing the cloud again after they are revoked. Finally implement this secure distribution scheme into group data sharing environments. To reduce the computation burden on the user side, a Third Party Auditor (TPA) is introduced to verify the integrity of the cloud data on behalf of user. When owner send request for file auditing, TPA will check the file integrity using TPA verification key and send results to the owner.*

**Keywords:** *Cloud computing ,Data sharing ,Security ,Privacy Data confidentiality ,Data integrity ,Access control,Third-party authentication ,Third-party verification ,Group-based access control ,Third-party auditor ,Symmetric key encryption ,Collusion attacks ,Replay attacks ,Security analysis ,Computation overhead ,Communication overhead.*

## 1.INTRODUCTION

The project focuses on ensuring that data shared between multiple users is protected against unauthorized access and tampering, while also allowing users to verify the integrity of the data. The project involves the use of various security mechanisms such as access control, encryption, and digital signatures to provide a secure data sharing environment. Access control mechanisms are used to ensure that only authorized users have access to the data, while encryption is used to protect the data from unauthorized access or interception during transmission. In addition to these mechanisms, the project also uses digital signatures to verify the integrity of the data. Digital signatures are used to ensure that the data has not been tampered with or altered in any way during transmission or storage. This provides an additional layer of security to the data sharing process. Overall, A Secure Data Sharing in Multi User Environment with

Integrity Verification project aims to provide a secure and reliable way for multiple users to share data in a way that is protected against unauthorized access and tampering. The project is relevant in various scenarios where multiple users need to access the same data, such as in a corporate or academic setting, and where data security is of utmost importance.

Managing and auditing network access is essential to information security. Access can and should be granted on a need-to-know basis. With hundreds or thousands of employees, security is more easily maintained by limiting unnecessary access to sensitive information based on each user's established role within the organization.

- Reducing administrative work and IT support
- Maximizing operational efficiency
- Improving compliance

**Reducing administrative work and IT support:** With RBAC, you can reduce the need for paperwork and password changes when an employee is hired or changes their role. Instead, you can use RBAC to add and switch roles quickly and implement them globally across operating systems, platforms and applications. It also reduces the potential for error when assigning user permissions. This reduction in time spent on administrative tasks is just one of several economic benefits of RBAC. RBAC also helps to more easily integrate third-party users into your network by giving them pre-defined roles.

**Maximizing operational efficiency:** RBAC offers a streamlined approach that is logical in definition. Instead of trying to administer lower-level access control, all the roles can be aligned with the organizational structure of the business and users can do their jobs more efficiently and autonomously.

**Improving compliance:** All organizations are subject to federal, state and local regulations. With an RBAC system in place, companies can more easily meet statutory and regulatory requirements for privacy and confidentiality as IT departments and executives have the ability to manage how data is being accessed and used. This is especially significant for health care and financial institutions, which manage lots of sensitive data such as PHI and PCI data.

## 2.RELATED WORK

**TITLE: A Comprehensive Review on Secure Data Sharing in Cloud Environment**
**AUTHOR: Sita Kumari Kotha**

This paper analyzed though it's a popular IT buzzword and concepts are derived from decade old grid computing, distributed computing, utility computing and intensive application computing. It offers a broader range of services such as virtual machines (VMs), servers, storage devices, operating systems (OS), and network resources over the internet to its users on 'pay-for-usage' basis. Dynamic group data sharing were users anonymously share his/her data with other group members over cloud could compromise security hence there is need to design an efficient, secure data sharing in dynamic group. Hence, this review paper presents various problems and challenges in designing an effective dynamic group data sharing. The problems and challenges are classified based on Client based and service provider based were client-based problems includes user authentication, user privacy and security, data confidentiality & integrity and query cost and service provider based problems includes user's identity & traceability, user revocation, energy efficiency and performance. Based on the challenges, researchers have proposed and developed various protocols, management and control mechanisms under data security, access control, query grouping and energy efficiency headings which is briefly summarised in this review to help future researchers in developing efficient, security data sharing schemes in cloud environment.

**TITLE: Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System**
**AUTHOR: OSAMA AHMED KHASHAN**

In this work, we aim to design a system that allows users to accomplish a secure data storage and secure data sharing of outsourced data in untrusted cloud environments. Our system design should achieve the following goals: Data confidentiality and integrity: the designed OutFS must encrypt data at user-side before being stored to synchronized cloud storage, using robust encryption algorithms and strong encryption keys.

Files stored at the cloud should remain encrypted during any operation, and their integrity is protected from unauthorized change or tampering. Data sharing: the ability to securely share data amongst users is essential in our work. Data owners can easily perform data sharing with other users without revealing any sensitive information, and without relying on the cloud mechanisms to authenticate remote users. Transparency: the system should allow users to work on plaintext files without encryption when they access files stored on their devices. The file system must transparently encrypt and decrypt all synchronized files to a directory on the cloud, so that the user should not notice any difference in using the third- party cloud storage. Efficiency, scalability, and applicability: the designed system must support users in the local and remote domains. It should be highly efficient and scalable to handle the complexity in key management and computations when data is shared between large numbers of users. In the meantime, the efforts of data owners to manage the users and keys should be reduced.

**TITLE: A Parallel and Forward Private Searchable Public-Key Encryption for Cloud-Based Data Sharing**
**AUTHOR: BIWEN CHEN**

In this paper, data sharing through the cloud is flourishing with the development of cloud computing technology. The new wave of technology will also give rise to new security challenges, particularly the data confidentiality in cloud-based sharing applications. Searchable encryption is considered as one of the most promising solutions for balancing data confidentiality and usability. However, most existing searchable encryption schemes cannot simultaneously satisfy requirements for both high search efficiency and strong security due to lack of some must-have properties, such as parallel search and forward security. To address this problem, we propose a variant searchable encryption with parallelism and forward privacy, namely the parallel and forward private searchable public-key encryption (PFP-SPE). PFP-SPE scheme achieves both the parallelism and forward privacy at the expense of slightly higher storage costs. PFP-SPE has similar search efficiency with that of some searchable symmetric encryption schemes but no key distribution problem. The security analysis and the performance evaluation on a real-world dataset demonstrate that the proposed scheme is suitable for practical application. We design a parallel and forward private SPE scheme (PFP-SPE) following the hidden data structure used by Xu, but with a very different implement. PFP-SPE uses a hidden star-chain data structure, in which every update generates a new state, which is like the pointer that points all the newly inserted files and the states are related by a symmetric key primitive. The search server can only decrypt the previous states by the current state and the corresponding key and then finds all matching files, but it can not predict the next state.

**TITLE: A Novel Structure-Based Data Sharing Scheme in Cloud Computing**
**AUTHOR: Huiyao ZHENG**

In this paper, an anonymous and traceable data sharing scheme in cloud computing is proposed. The main contributions of this paper are listed as follows. • A effective session key agreement protocol is proposed. In this paper, a based on matrix structure session key agreement protocol is design. By two-part calculation, a group key can be derived used for data sharing in cloud. Moreover, the matrix structure can reduce the communication cost. • Anonymity and traceability are supported in data sharing scheme. Anonymity is ensured by using phony-ID in this paper, which can protect the user’s real identity. When a user uploads irrelevant information to cloud, the trusted third party can trace the real identity even though the user uses phony-ID sharing data. The users’ privacy and the system security are guaranteed due to anonymity and traceability. • The authentication of the message is satisfied. In this paper, each message is verified by receiver in session key generation phase, which ensures the correctness of the session key and ciphertext. The authenticated message can derive symmetric key used in encrypted the shared data. In the proposed scheme, first, users need obtain a valid identity from TTP. Then, the group members generate a session key based on the matrix structure in order to ensure secure data sharing. After that, uploader adopts symmetric encryption algorithms using the session key to encrypt the message and upload the ciphertext to cloud. All users in cloud can download the ciphertext message; however, they cannot decrypt the data

**TITLE: Group Key Management Protocol for File Sharing on Cloud Storage**
**AUTHOR: SHOUYI ZHANG**

In this paper, we proposed a secure group key management protocol on cloud storage over unreliable channels, aiming at protecting the shared files on the cloud storage. Mixed encryption technology is used to generate and distribute group keys, which resistance attacks from network monitor. In addition, we propose a verified protocol that against the attacks from the file sharers or the cloud provider. Faced with today’s innovative blow-up of cloud technologies, rebuilding services in terms of cloud have become more popular. In a shared-tenancy cloud computing environment, data from different clients which can be hosted on separate virtual machines may reside on a single physical machine. Under this paradigm, the data storage and management is under full control of the cloud provider, so data owners are left vulnerable and have to solely rely on the cloud provider to protect their data. Recent news shows that Google provided the FBI all the documents of one of its users after receiving a search warrant, but the users have not been aware of the search until they are arrested. Because cloud provider has the full access to the data, the privacy of data could be violated if user's data is intercepted or modified by the cloud provider. Our general goal is to develop an efficient group key management protocol for file sharing on cloud storage; the resulting techniques should be able to confront two main problems. One is ensuring that the content of the shared files cannot be learned by the unauthorized peoples. The other is protecting the files against misoperation by the cloud provider and interception by the network.

## 3.EXISTING SYSTEM

Propose an attribute-based controlled collaborative access control scheme for public cloud storage. Restrict user collaboration in the same group that corresponds to the same project for which the involved people are responsible. Thus, in proposed work, in order to provide both data confidentiality and collaborative access control, only people who are in charge of the same project are allowed to collaborate. Technically, data owners allow expected collaboration by designating translation nodes in the access structure. In this way, unwanted collusion can be resisted if the attribute sets by which users are collaborating are not corresponded to translation nodes. For each translation node, an additional translation value is generated. Using this translation value and special translation keys embedded in users' secret keys, users within the same group can collaborate to satisfy the access structure and gain the data access permission. For colluding users across groups, their access is not permitted as their secret keys do not correspond to the same group. Users are divided into groups in a way such that the collaboration is restricted and secure. That is to say, only users responsible for the same project are allowed to collaborate in case those malicious users who are not responsible for the project collude. Extensive security analysis is given to show the security properties of our proposed scheme.

In existing scheme, the security assumptions of the four roles can be defined as follows. Cloud servers are always online and are managed by the cloud provider who is usually assumed to be "honest-but-curious". It means that cloud servers will correctly execute the tasks assigned to them for profits, but they would try to obtain as much secret information as possible based on data owners' inputs and outsourced data.

**DISADVANTAGES :**

- Additional secure channel is essential for the key authority to transmit new keys.
- This scheme only suitable for selective problems.
- Cannot resist against collusion of malicious users.
- The system had a heavy key distribution overhead

## 4.PROPOSED SYSTEM

To enable data sharing in the Cloud, it is essential that only authorized users are able to get access to data stored in the Cloud. When the data owner wants to share their own data to a group, he/she sends the key used for data encryption to each member of the group. Any of the group members can then get the encrypted data from the Cloud and decrypt the data using the key and hence group member does not require the interference of the data owner. The problem in this technique is that it is inefficient. When the data owner gets back the access rights from a member of the group, that member must not be able to access to the corresponding data. Since the unauthorized member of the group still has the data access key. So the data owner has to re-encrypt the data with a new key. When the data is re-encrypted, data owner must give out the new key to the remaining users in the group and this is computation inefficient.

This proposed work also concentrate an identifying misbehave data access in cloud environment using Data auditing scheme. Data sharing as one of the most common features in cloud storage, allows a number of users to share their data with others. However, these shared data stored in the cloud might contain some sensitive information. In remote data integrity auditing schemes, the data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures are used to prove the cloud truly possesses these data blocks in the phase of integrity auditing. And then the data owner uploads these data blocks along with their corresponding signatures to the cloud. To overcome the problems present in the existing auditing scheme here propose an efficient integrity auditing with the help of third party auditor.

**ADVANTAGES :**

- Only one user with a satisfied attribute set with their role can access the data.
- The secret key, together with user's roles, determines whether the user satisfies the policy.
- Can extract the original data of a user during the auditing process.

## 5. Methodology

### A. AES Encryption

The AES cipher is also referred to as the block cipher. Now a successful attack has been noted on AES. Some advantages of AES are smooth to enforce on eight-bit processors and powerful implementation on 32-bit structure processors. AES encryption is performed in multiple rounds. Each round has 4 vital steps in conjunction with sub-byte, shift row, mix column, and upload round key. Sub-byte is the substitution of bytes the use of a lookup-up table. Shift row is the shifting of rows consistent with byte duration. The Mix column is multiplication over the Galois subject matrix. Finally, inside the upload round key step, the output matrix of the blend column is XORed with the round key. The wide variety of rounds used for encryption is predicated upon at the critical issue size. For a 128-bit key, these 4 steps are applied to 9 rounds, wherein the 10th round does not take into account the aggregate column step. Since all steps are recursive, decryption is the alternative of encryption.

### B. Algorithm Procedure

The set of regulations begins with an Add round key diploma observed via the usage of 9 rounds of 4 degrees and the tenth round of 3 ranges. This applies for each encryption and decryption with the exception that each degree of spherical the decryption set of policies is the inverse of its counterpart in the encryption set of rules. The four ranges are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The 10th spherical in reality leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm include the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round leaves out the Inverse Mix Columns degree. Each of those degrees will now be taken into consideration in extra element.

### C. Procedure

**1) Data Sharing Framework**

In this module, create a local Cloud and provide priced abundant storage services. The group managers can add their data within the cloud, wherein the cloud storage can be made at ease. However, the cloud is not fully dependent on by users for the reason that CSP is very probably to be outside of the cloud customers depended on the area. The Proposed

secure data sharing framework provides communication between the group manager and the group members. Group Manager takes charge of followings,

1. System parameters generation
2. User registration
3. User revocation
4. Revealing the original identity of the outsourced group manager.

Therefore, the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager should login and upload each and every file in the cloud. The group manager is responsible for every user registration and user revocation too. *2) Key Generation and Distribution*

Key Generation is the process of generating a secret key for group manager and group members. After completion of the registration secret key is generated using a random key generation process and send to the corresponding member through email. During login, a member should enter their secret key that will be verified with the database. If a member does not have valid user id they will not allow accessing an application. The concept of group signatures was performed by PKG (Public Key Generation). Informally, a group signature scheme permits any member of the group to sign messages even as retaining the identity secret from verifiers. Besides, the certain institution manager can reveal the identity of the signature's originator when a dispute happens, which is denoted as traceability. In this paper, a variant

of the group signature updation scheme will be used to achieve anonymous access control, as it supports efficient membership revocation.

**3) Data Upload with Encryption**

The Group manager is a cloud client who registers with the CSP (Cloud Service Provider). The Manager outsources data to the cloud in an encrypted form. Group Manager anonymously gets authenticated to the cloud while getting duly authenticated. It is the duty of the Group manager to prevent the admission of malicious group manager's to the cloud. The encrypted data is uploaded to the cloud by the group manager. The group manager can encrypt the file using the AES encryption technique. The choice of encryption is of the group manager.

**4) Data Access**

Members must be authenticated to access the service from the cloud. The commonly used security mechanism for data access is to check the username and password pair. Member provides the username and password to the cloud server and then the cloud server checks the authenticity of members. If a member is authorized by a service provider will allow a member to search the file from the cloud otherwise the member will not be allowed to search files. Member can be extracting the stored data anywhere from cloud storage. If a new member is added to the group, this system can be granted access to the file and sharing the group key to the added member wherein he can directly download the decrypted data file, when they are downloading the file a secret key is generated and sent to their own mobile number, using that key member can download the data.

**5) User Revocation**

User revocation is performed by the group manager through a public revocation list, It supported by which group manager can encrypt the info files and makes sure the confidentiality against the revoked members. Revoked customers are not able to decrypt the data moved into the cloud after the revocation. The remaining members need to update their group keys to avoid unwanted data access made by removed members. New granted users can get present group keys and learn all the content data files stored by the group manager.

**6) Data Auditing**

A public verifier, like a third-party auditor (TPA) providing expert data auditing services or a knowledge user outside the group meaning to utilize shared data, is in a position to publicly verify the integrity of shared data stored within the cloud server. When a public verifier wishes to see the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the cloud server responds to the general public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the whole data by verifying the correctness of the auditing proof. Essentially, the method of public auditing may be a challenge and-response protocol between a public verifier and therefore the cloud server.

**D. Data Sharing Framework**

Data sharing between two members or group of members take several issues into account. Only records Manager and the participants access the data, here no others can access the records inclusive of the Cloud Service Provider. The records of the manager get lower back the permission to give admission to records for any member of the organization.

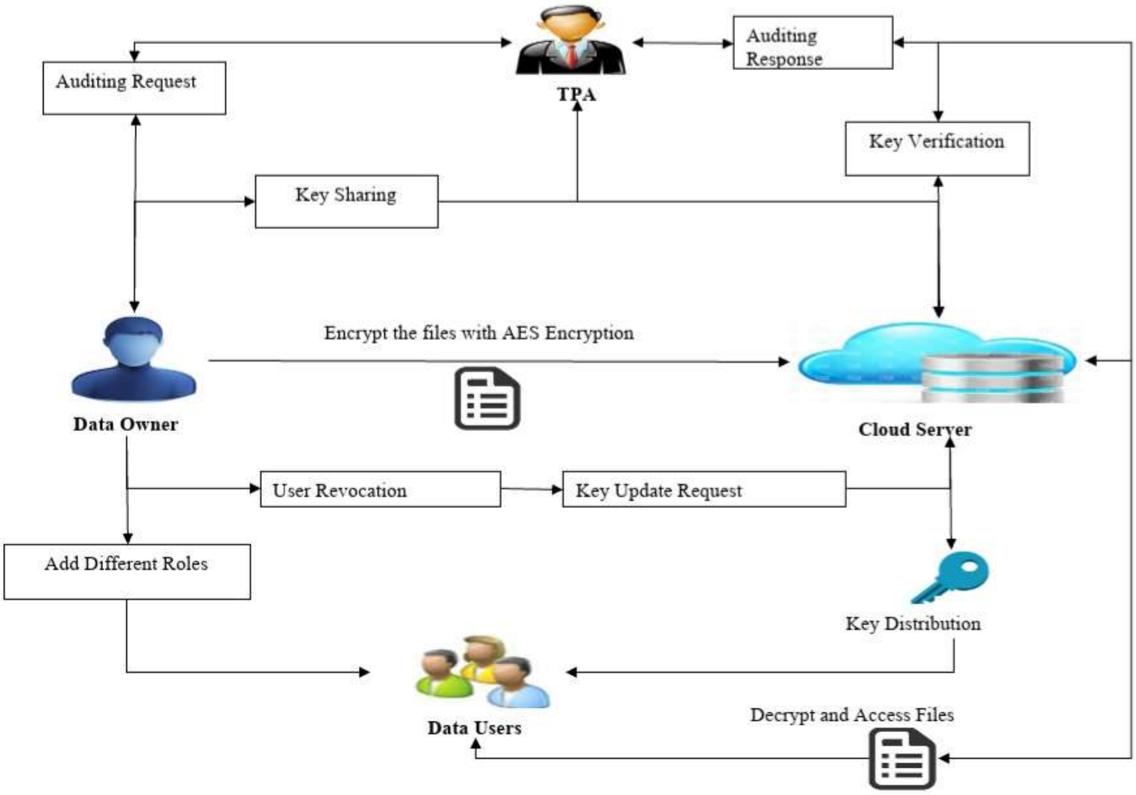


Fig. 1. Architecture for proposed work

The manager can upload a new member to the group. The group manager can specify a group of members who can be authorized to view his or her data. Any time the member of the organization has to access the data without the group manager’s interference. The member of the organization ought to no longer be allowed to revoke the rights of different participants of the organization or add new members to the organization. Secure user revocation means the revoked members cannot get the original data file even if they conspire with the untrustworthy cloud.

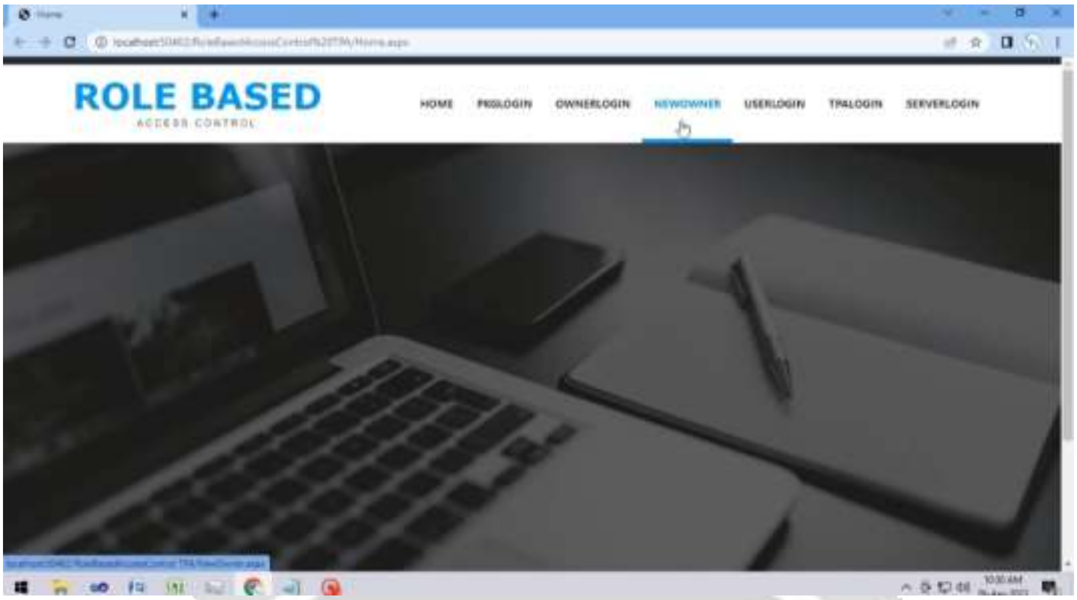
The group manager has to specify who has read/write permissions at the facts manager’s files. To protect data confidentiality, to approach encrypt data files before uploads the encrypted data into the cloud is a challenging task inactive groups in the cloud. This scheme can achieve fine-grained access control. It provides security against a

collusion attack by using a group signature that provides secure user revocation. Collusion attack means decryption of data by a revoked user using his secret key and gets a top-secret file by conspiring with the cloud.

This method achieves secure key distribution, fine-grained access control, anti-collusion attack, and secure user revocation.

## 6.Experimental Result

The Experimental result shows the overall performance of the proposed system. Here Role-based access control for data sharing and auditing schemes are implemented using ASP.NET as front end and SQL as back end software. This will help to improve file security.



The above figure is interface of a secure group data sharing

## 7. CONCLUSION

Data sharing in the Cloud is available in the future as demands for data sharing continue to grow rapidly. Proposed work, presented a review on secure data sharing in cloud computing environment. To reduce the cost data owner outsource the data. Data owner is unable to control over their data, because cloud service provider is a third party provider. The problem with data sharing in the cloud is the privacy and security issues. Various techniques are discussed in this paper to support privacy and secure data sharing such as AES encryption, Group data sharing and User revocation. The study concludes that secure anti-collision data sharing scheme for groups provides more efficiency, supports access control mechanism and data confidentiality to implement privacy and security in group sharing.

## 8.REFERENCE

[1] Kotha, Sita Kumari, Meesala Shobha Rani, Bharat Subedi, Anilkumar Chunduru, Aravind Karrothu, Bipana Neupane, and V. E. Sathishkumar. "A comprehensive review on secure data sharing in cloud environment." Wireless Personal Communications 127, no. 3 (2022): 2161-2188.
[2] Khashan, Osama Ahmed. "Secure outsourcing and sharing of cloud data using a userside encrypted file system." IEEE Access 8 (2020): 210855-210867.
[3] Chen, Biwen, Libing Wu, Li Li, Kim-Kwang Raymond Choo, and Debiao He. "A parallel and forward private searchable public-key encryption for cloud-based data sharing." IEEE Access 8 (2020): 28009-28020.
[4] Zheng, Huiyao, Jian Shen, Youngju Cho, Chunhua Su, and Sangman Moh. "A Novel Structure-Based Data Sharing Scheme in Cloud Computing." IEICE TRANSACTIONS on Information and Systems 103, no. 2 (2020): 222-229.
[5] Zhang, Shouyi, Si Han, Baokun Zheng, Ke Han, and Entong Pang. "Group key management protocol for file sharing on cloud storage." IEEE Access 8 (2020): 123614123622.
[6] Xu, Yang, Cheng Zhang, Guojun Wang, Zheng Qin, and Quanrun Zeng. "A blockchainenabled deduplicatable data auditing mechanism for network storage services." IEEE Transactions on Emerging Topics in Computing 9, no. 3 (2020): 1421-1432.
[7] Zhang, Jiawei, Teng Li, Mohammad S. Obaidat, Chi Lin, and Jianfeng Ma. "Enabling efficient data sharing with auditable user revocation for IoV systems." IEEE Systems Journal 16, no. 1 (2021): 1355-1366.

[8] Bove, Davide, and Tilo Müller. "Investigating characteristics of attacks on public cloud systems." In 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 89-94. IEEE, 2019.
[9] Yang, Xiaodong, Xizhen Pei, Meiding Wang, Ting Li, and Caifen Wang. "Multi-replica and multi-cloud data public audit scheme based on blockchain." IEEE Access 8 (2020): 144809-144822.
[10] Zhang, Cheng, Yang Xu, Yupeng Hu, Jiajing Wu, Ju Ren, and Yaoxue Zhang. "A blockchain-based multi-cloud storage data auditing scheme to locate faults." IEEE Transactions on Cloud Computing 10, no. 4 (2021): 2252-2263.