International Journal of Research in Engineering, Science and Management
Volume-3, Issue-7, July-2020
journals.resaim.com/ijresm | ISSN (Online): 2581-5792

Enabling Secure Data Sharing Scheme in Cloud Storage Group by Verify Using Third Party Authentication

M. Jenifa[1*], K. Ambika[2]
[1]*PG Scholar, Department of Computer Science and Engineering, Anna University, BIT-Campus, Tiruchirappalli, India*
[2]*Assistant Professor, Department of Computer Science and Engineering, Anna University, BIT-Campus, Tiruchirappalli, India*
*Corresponding author: jenifa.m.l.abish93@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 management by drifting the local management 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 management. Data confidentiality becomes the main concern in outsourcing client data to cloud storage. It is also essential for an access control mechanism for preventing data mistreatment within the organization. Unfortunately, it is hard to design cozy and green facts sharing scheme, particularly for dynamic groups within 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 the existing group and no need to encrypt again the original data. Any member in the group can use the source within the cloud and revoked members can't access the cloud once more after they are revoked. Finally, implement this secure distribution scheme into group data sharing environments. To reduce the computation burden on the member side, a Third Party Auditor (TPA) is introduced to verify the integrity of the cloud data on behalf of the member. When the manager sends a request for file auditing, TPA will check the file integrity using the TPA verification key and send results to the manager.**

***Keywords*: Secure Data Sharing, Role with Time based access control, AES encryption, Group member revocation, Key Updation, Data Auditing, TPA Verification.**

1. Introduction

A. Cloud Computing Basics

Cloud computing technology consists of the use of computing resources that are delivered as a service over a network. In cloud computing model users should provide access permission to their records for storing and performing the business operations. Hence cloud providers need to provide trust and safety, as there's precious and sensitive information in large amounts stored on the clouds. There are worries about flexible, scalable and quality grained access control inside the cloud computing.

Cloud computing is consistently growing and there are many main cloud computing providers including Amazon, Google, Microsoft, Yahoo, and many others who are offering solutions including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a-Service and Infrastructure-as-a-Service (IaaS). In addition, considering the possibility of substantially minimizing expenses by optimization and also maximizing operating as well as economic effectiveness, cloud computing is an excellent technology. Furthermore, cloud computing can tremendously boost its cooperation, speed, and also range, thus empowering a completely worldwide computing model on the web infrastructure.

Cloud computing handles useful resource management in a higher way for the reason that consumer does not needs to be responsible for figuring outsources for storage. If a person wants to save more records they request it from the cloud provider and as soon as they may be completed they could both release the storage with the aid of virtually stopping the use of it, or move the data to a protracted-term lower-cost storage resource. The data now not want to difficulty themselves with storage and cost that accompany new and old sources.

Cloud computing service models are all inside in the cloud sing and laptops, desktops, phones, and tablets act as clients to get services from the cloud. Servers provide services to clients consistent with their request or pay base. Cloud

computing provides a shared pool of configurable IT resources on-demand, which needs the minimal effort of management to get better services. Services are based on various Service Level Agreement between service providers and consumers.

B. Cloud Security

The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information.

The intrinsic problems of data security, governance, and control with control inside the cloud computing are discussed. The key protection, privateness, and true issues within the existing environment of cloud computing and assist customers to know the tangible and intangible threats related to its use. According to the authors, there are three essential ability threats in cloud computing, particularly, security, privateness, and trust. Security performs a critical role inside the current technology. It divided into further types called protection approaches, server tracking or tracing, data confidentiality, and avoids malicious insider's illegal operations and carrier hijacking.

An information security framework for cloud computing networks is proposed. The authors especially mentioned the security issues associated with cloud information storage. There are also some patents approximately the statistics storage safety techniques. Give a survey on secure cloud computing for essential infrastructure. A security and privacy framework for RFID in cloud computing was proposed for RFID technology integrated into cloud computing, which will combine cloud computing with the Internet of Things.

C. Data Integrity

Data integrity is one of the maximum crucial elements in any information storage. Generally, data integrity defines defensive statistics from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific organization resources guarantees that precious records and services are not abused, misappropriated, or stolen.

Data integrity is without difficulty executed in a standalone gadget with a single database. Data integrity in the standalone system is maintained via database constraints and transactions, which is usually finished by a database management system (DBMS). Transactions ought to observe ACID (atomicity, consistency, isolation, and durability) properties to ensure the integrity of data. Most databases help ACID transactions and might maintain information integrity.

Authorization is employed to regulate the access to knowledge. It is the mechanism through which a device determines what stage of access permission to a selected authenticated person should must comfortable resources managed by way of the system.

D. Data Confidentiality

Data confidentiality is crucial for customers to store their personal or private information inside the cloud. Authentication and access permission techniques are used to make certain data confidentiality. Data confidentiality, authentication, and access to manipulate issues in cloud computing will be addressed with the aid of growing cloud reliability and trustworthiness. Because the users do no longer accept as true with the cloud providers and cloud storage service carriers are absolutely not possible to remove ability insider danger, it is very risky for users to save their sensitive records in cloud storage immediately. Simple encryption is faced with the important thing management problem and cannot guide complex necessities along with the query, parallel change, and fine-grained authorization.

E. Data Availability

Data availability defined as, while accidents such as hard disk damage, IDC fire, and network failure problem occur, the volume that person's records may be used or recovered and how the users affirm their data by using strategies rather than depending at the credit assure by means of the cloud service company on my own. The problem of storing information over the transmission boarder servers is an extreme difficulty of customers due to the fact the cloud companies are ruled by using the local laws and, consequently, the cloud customers must be cognizant of these laws. Moreover, the cloud provider should make the security of the records, particularly records confidentiality and integrity. The cloud companies need to share all such concerns with the consumer and construct agree with the relationship in this connection. The cloud vendors need to offer guarantees of records protection and give an explanation for the jurisdiction of local laws to the clients. The most important focus of the paper is on the ones records troubles and challenges which can be related to the data storage area and its relocation, price, availability, and safety.

F. Data Privacy

Privacy is defined as the person or organization’s ability to secure their details or information about themselves and thereby monitor their activities. In the cloud, the privacy method defines when users visit the sensitive data, the cloud services can prevent a potential adversary from inferring the person's conduct through the person's visit model (no longer direct facts leakage). Researchers have centered on Oblivious RAM (ORAM) generation. ORAM technology visits numerous copies of information to hide the real visiting targets of users. ORAM has been broadly used in software protection and has been utilized in protecting privacy in the cloud as a promising era.

2. Related Work

Wenting Shen, et. al. [1] proposes a remote data integrity auditing scheme that realizes data sharing by hiding sensitive

information. In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of files and transforms these data block's signatures into valid ones of sanitized files. These signatures are used to verify the integrity of the sanitized files in the phase of integrity auditing. As a result, this scheme makes the file stored in the cloud able to be shared and used by others in the condition. The sensitive information is hidden, while the remote data integrity auditing is still efficiently executed.

Li, et al. [2] propose efficient auditing using key updating and authenticator-evolving mechanism of the files for secure cloud data auditing, which incorporates proxy re-signatures and homomorphic linear authenticators. When the cloud user needs to update his key, instead of downloading the entire file and re-generating all the authenticators, the user can simply download one single file tag, workout a re-signing key with a new private key and upload new file tag together with some verification of data to the cloud server. TPA is responsible for checking the integrity of the cloud data on behalf of cloud users. In this case, they have no time, feasibility to monitor their data, and return the auditing report to the cloud user.

Zhu, et al. [3] The attack on mona, proposed a secure multi-owner data sharing scheme. This scheme can attain fine-grained access control and revoke users who will not be able to access the sharing data again once they are revoked. However, the scheme will easily suffer from the collusion attack by the revoked user and the cloud.

Liu, et al. [4] proposed a secure multi-owner data sharing scheme, named mona. The revoked user can use his private key to decrypt the encrypted data and get the secret data after his revocation through conspiring with the cloud. In the phase of document access, the revoked user sends his request to the cloud, and then the cloud responds to the corresponding encrypted records file. After that, the revoked user can compute the decryption key with the help of the attack algorithm. At last, this attack can cause the revoked users to get the sharing data and disclosing other secrets of legitimate members.

Zhou, et al. [5] proposed a secure access control scheme on encrypted data in cloud storage space by invoking a role-based encryption technique. This method can achieve well-organized user revocation that combines role-based access control policies with encryption to secure huge data storage space in the cloud. Unfortunately, verification between entities is not afraid. The method easily suffers from attacks, for example, a collusion attack. At last, this attack can direct to disclosing sensitive data files.

Guangyang Yang, et. al. [6] propose an efficient public auditing solution that can preserve the identity privacy and the identity traceability for group members simultaneously. Specifically, we first design a new framework for data sharing in the cloud and formalize the definition of the public auditing scheme for shared cloud data supporting identity privacy and traceability. And then we construct such a scheme, in which a group manager is introduced to help members generate authenticators to protect identity privacy and two lists are employed to record the members who perform the latest modification on each block to achieve identity traceability. Besides, the scheme also achieves data privacy during the authenticator generation by utilizing a blind signature technique.

Zhang, et. al. [7] proposes a novel storage auditing scheme that achieves highly-efficient user revocation independent of the total number of file blocks possessed by the revoked user in the cloud. This is achieved by exploring a novel strategy for key generation and a new private key update technique. Using this strategy and the technique, we realize user revocation by just updating the non-revoked group user's private keys rather than authenticators of the revoked user. The integrity auditing of the revoked user's data can still be correctly performed when the authenticators are not updated. Meanwhile, the proposed scheme is based on identity-base cryptography, which eliminates the complicated certificate management in traditional Public Key Infrastructure (PKI) systems.

Shen, et. al. [8] proposes an efficient data auditing protocol with a blockless verification scheme as well as batch auditing. The novel dynamic structure in the proposed protocol has a doubly linked info table and a location array. The doubly linked info table (DLIT) is a two-dimensional data structure employed by the TPA to store data information concerning auditing, differing from the one-dimensional Index Hash Table (IHT). we use the concatenation of the user ID and file ID to identify each file, making the unique identifier much easier to find. The right part is the block information, including the current version number and the time stamp, which are generated when a given block is uploaded or updated.

Shen, et. al. [9] proposed a cloud storage auditing scheme for group users, which greatly reduces the computation burden on the user side. In this scheme, they introduce a Third Party Medium (TPM) to perform time-consuming operations on behalf of users. The TPM in charge of generating authenticators for users and verifying data integrity on behalf of users. In order to protect the data privacy against the TPM, we blind data using simple operations in the phase of data uploading and data auditing. The user no need to perform time-consuming decryption operations when using cloud data. We set an expiration time of the authorization to make sure that the TPM who possesses the authorization within a valid period is able to upload data to the cloud and challenge the cloud data.

Yun Xue Yan, et. al. [10] proposed a secure and effective data sharing scheme for dynamic user groups. In order to realize the user identity tracking and the addition and deletion of dynamic group users, we add a new role called Rights Distribution Center (RDC) in our scheme. To protect the privacy of user identity, when performing a third-party audit to verify data integrity, it is not possible to determine which user is a specific user. Therefore, the fairness of the audit can be promoted. Define a new integrity audit model for shared cloud data. In this scheme, the user sends the encrypted data to the

cloud and tag the data to the Rights Distribution Center (RDC) by using data blindness technology.

3. Existing Methodologies

Cloud storage is one of the most important services in cloud computing, which enables the interconnection of all types of electronic products. Group data sharing has many practical applications, such as electronic health networks, wireless body area networks, and electronic literature in libraries. There are two ways to share data in cloud storage. The second refers to a many-to-many pattern, this defines a situation in which many clients in the common group should authorize access to their data for many clients at the same time.

A. Identity Based Encryption

In existing work, implementing revocable-storage identity-based encryption (RS-IBE), this provides the forward /backward security of ciphertext by introducing additional functionalities of user revocation and ciphertext update simultaneously.

B. IBE

Identity Based Encryption (IBE) takes an effective approach to the problem of encryption key management. IBE can use any string as a public key, enabling data to be protected without the need for certificates. Identity-based systems allow any member to generate a public key from a known identity value such as an ASCII string. A trusted third party is denoted by a Private Key Generator (PKG) that generates the corresponding private keys. The PKG first provides a master public key, and then provide the corresponding master private key. Given the master public key, any member can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To acquire a corresponding personal key, the user authorized to apply the identity ID contacts the PKG, which uses the master key to generate the personal key for Identity ID. Thus, members may additionally encrypt messages without an earlier distribution of keys among individual contributors. This is useful in instances wherein the pre-distribution of authenticated keys is inconvenient due to technical restraints. However, to decrypt or sign messages, the authorized person must achieve the ideal personal key from the PKG.

C. RS-IBE

The non-revocable data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. The process of decrypt and then re-encrypt necessarily involves the member's secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the effect of the secret key needs to be restrained to the best common decryption, and it is inadvisable to replace the cipher textual content periodically through the usage of the secret key. Another challenge comes from efficiency. To update the ciphertext of the shared data, the data provider has to frequently carry out the procedure of download-decrypt and re-encrypt-upload. This process brings great communication and computation cost and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage.

4. Secure Group Data Sharing with User Revocation

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. Figure 4.1 demonstrates the Secure Group Sharing in Cloud. When the group manager desires to share their data into a group, he/she sends the secret key used for data encryption to every member of the organization. Any of the institution participants can then get the encrypted data from the Cloud and decrypt the information using the secret key and for this reason group member does now not require the interference of the Group Manager. The hassle in this approach is that it's far inefficient. When the group manager receives back the access rights from a member of the institution, that member has to no longer be capable of access to the corresponding data. Since the unauthorized member of the organization now also has the data access key. So the Group Manager has to change the key using the process of re-encrypt the data. When the data is re-encrypted, the group manager must give out the new key to the remaining customers in the group and that is computation inefficient.

This proposed work also concentrates an identifying misbehave data access in a cloud environment using a Data auditing scheme. Data sharing as one of the most common features in cloud storage, allows a number of members to share their data with others. In remote data integrity auditing schemes, the group manager firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures used to prove the cloud truly possesses the data blocks in the phase of integrity auditing. And then the group manager 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 a third-party auditor.

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.

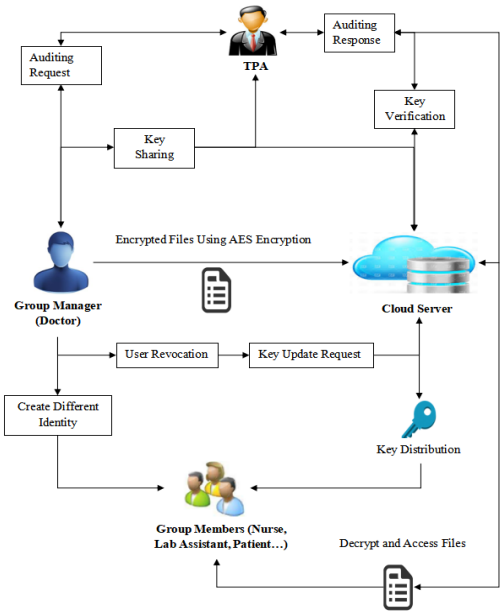

Fig. 1. Architecture for proposed work

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.

A. New Doctor Registration

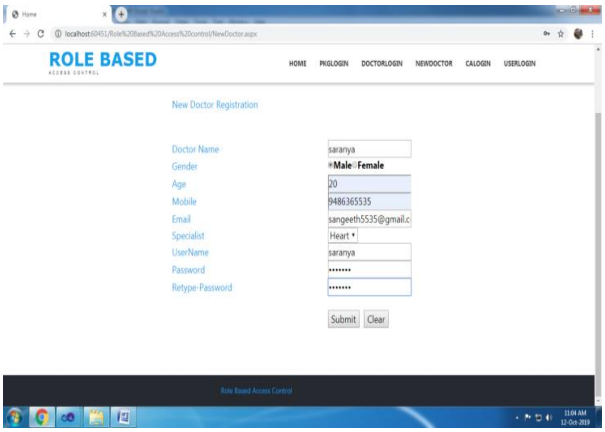

Fig. 2. New Doctor Registration

The Above figure shows the process of new doctor registration. Doctors are considered as group manager and they could register and get permission from the cloud to access and share data through the cloud.

B. Patient Registration

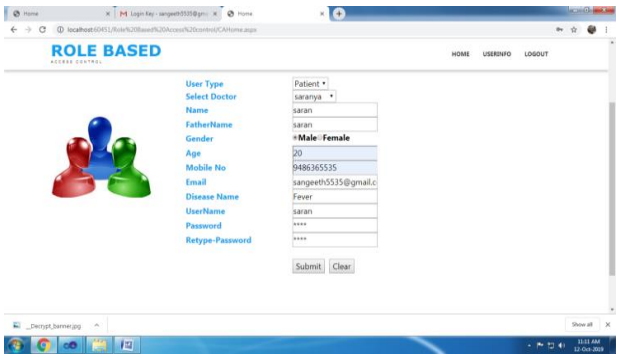

Fig. 3. Patient registration

This figure shows the process of entering patient details. Central Authority has permission to add patient details and allocate patients to the specified doctors. Patients are

considered as group members.

C. File Upload

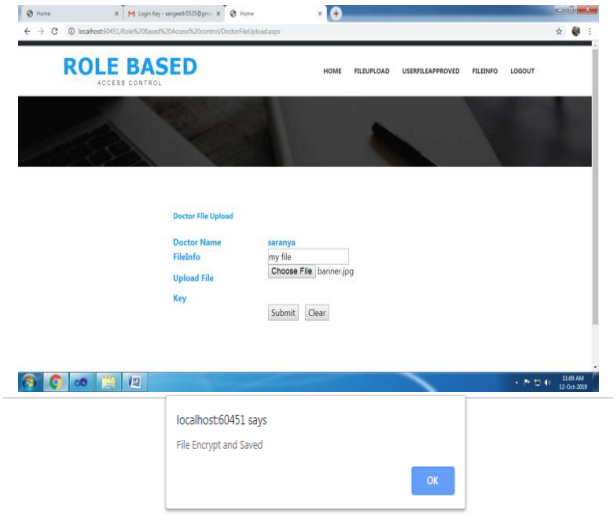

Fig. 4. File Upload

Above figure shows the process of file uploading. In this process group manager can upload files to share. Uploaded files get encrypted and stored on the server.

D. Key Verification and File Download

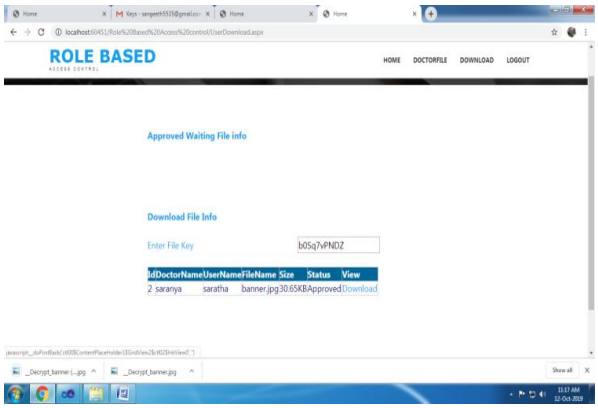

Fig. 5. Key verification and file download

This figure shows the process of file downloading and key verification. After verification of shared secret keys, group members can get files in decrypted format.

E. User Revocation

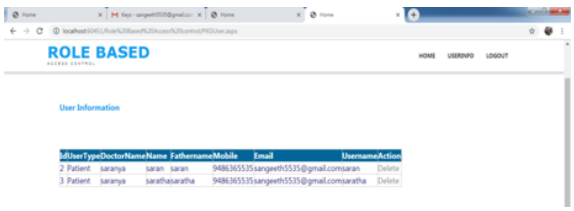

Fig. 6. Remove user

This figure shows the user revocation process. Central Authority has permission to remove members from the group.

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 the cloud computing environment. To reduce the cost group manager outsources the data. The group manager is unable to control their data because the 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 a secure anti-collusion data sharing scheme for groups provides more efficiency supports access control mechanisms and data confidentiality to implement privacy and security in group sharing. Proposed mechanisms also provide efficient integrity auditing of shared data, user revocation, and support batch auditing. TPA wouldn't learn any knowledge about the info content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious auditing task but also reduce the user's fear of their outsourced data leakage.

References

[1] Wenting Shen, Jing Qin, Jia Yu, Rong Hao, and Jiankun Hu. Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage. IEEE Transactions on Information Forensics and Security, Vol. 14, no. 2, 2019.

[2] Li, Yannan, Yong Yu, Bo Yang, Geyong Min, and Huai Wu. Privacy-preserving cloud data auditing with an efficient-key update. Future Generation Computer Systems 78 (2018): 789-798.

[3] Zhu, Z., Jiang, Z., & Jiang, R. Attack on mona: Secure multi-owner data sharing for dynamic groups in the cloud. In Information Science and Cloud Computing Companion (ISCC-C), 2013(IEEE). International Conference on (pp. 213-218).

[4] Liu, X., Zhang, Y., Wang, B., & Yan, J. Mona: Secure multi-owner data sharing for dynamic groups in the cloud. IEEE transactions on parallel and distributed systems, 24(6), (2013).

[5] Zhou, L., Varadharajan, V., & Hitchens, M. Achieving secure role-based access control on encrypted data in cloud storage. IEEE transactions on information forensics and security, 8(12), (2013).

[6] Guangyang Yang, Jia Yu, Wenting Shen, and Qianqian Su. Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability. Information Engineering, Volume 113 (2015): page 130-139.

[7] Zhang, Yue, Jia Yu, Rong Hao, Cong Wang, and Kui Ren. Enabling efficient user revocation in identity-based cloud storage auditing for shared big data. IEEE Transactions on Dependable and Secure Computing, Volume: 17, Issue: 3 (2020).

[8] Shen, Jian, Jun Shen, Xiaofeng Chen, Xinyi Huang, and Willy Susilo. An efficient public auditing protocol with a novel dynamic structure for cloud data. IEEE Transactions on Information Forensics and Security 12, no.10, (2017): 2402-2415.

[9] Shen, Wenting, Jia Yu, Hui Xia, Hanlin Zhang, Xiuqing Lu, and Rong Hao. Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium. Journal of Network and Computer Applications 82 (2017): 56-64.

[10] Yun Xue Yan, Lei Wu, Wen Yu Xu, Hao Wang, and Zhao Man Liu. Integrity Audit of Shared Cloud Data with Identity Tracking. Security and Communication Networks, Volume 2019.