IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, May 2023

# Threshold Multi Keyword Search for Group Data Sharing in Cloud

**Aswin K[1], Divya Shree P. K[2], Dowmika C[3], Gayathiri K. S[4], Megala V[5]**
Department of Computer Science and Engineering[1,2,3,4,5]
Dhanalakshmi Srinivansan Engineering College (Autonomous), Perambalur, India

**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:** *Data Sharing in Cloud, Group Key Verification, Group Data Sharing, Role Based Access Control, AES Encryption, User Revocation.*

## I. INTRODUCTION

Access control is a security technique that regulates who or what can view or use sources in computing surroundings. It is a basic concept in protection that minimizes risk to the enterprise or organization. Access control can be manipulated into two categories namely physical and logical. Physical access to manipulate limits access to campuses, buildings, rooms and physical IT property. Logical access control limits connections to computer networks, files and data.Access control structures perform identification authentication and authorization of customers and entities through evaluating required login credentials that may consist of passwords, personal identity numbers (PINs), biometric scans, protection tokens or different authentication elements. Multifactor authentication requires more authentication factors, is regularly a critical part of layered protection to defend access to manipulate systems.The intention of access control is to reduce threat of unauthorized access to physical and logical structures. Access control is a fundamental thing of safety compliance programs that guarantees security technology and access control policy shield private records, consisting of client information.

Recently many companies have infrastructure that limit access to networks, computer systems, packages, files and sensitive information, such as individually identifiable data and intellectual data access.Access control structures are complicated and can be difficult to manipulate in dynamic IT environments that contain on-premises structures and cloud services. After some excessive-profile breaches, technology vendors have shifted faraway from single sign-on structures to unified access control, which offers access controls for on-premises and cloud environments.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, May 2023

### 1.1 BENEFITS OF ACCESS CONTROL

Interest in cloud-based access to manipulate has surged in recent years, attracting businesses of various sizes and throughout industries. For everybody who has been seen the benefits of cloud-based systems, that's hardly a surprise.From streamlined system management to pricing flexibility, cloud-primarily based access manipulates offers some very interesting characteristics while compared with conventional, on-premise structures. Some key examples are listed underneath.

**Accessibility from anywhere with an Internet connection**

While some conventional access control systems provide some remote connectivity, cloud systems are designed with mobile accessibility in thoughts. Authorized users can log into the relevant access to control app, web portal, or network to view or manage device interest. Aside from supplying convenience, this additionally enables customers to obtain alerts and take actions in the event of an incident or emergency.

#### 1.1.2 Flexible cost management

Whereas conventional access control systems frequently include high upfront installation and equipment costs, cloud based services offer lots more flexibility in pricing. Instead of buying online equipment outright, users can prefer to lease equipment from an authorized reseller, avoiding high capital expenditure charges in prefer of modest ongoing operational expenses.

#### 1.1.3 Reduced burden on user staff

Maintaining a business service takes time and effort, especially for undertaking-critical ones like access control. By turning over the hosting and renovation of on-web site PCs, servers, facts-redundancy infrastructure and associated processes to the integrator, customers can dramatically decrease the weight on their very own IT personnel. Depending on the software itself, a cloud based system can reduce burden of IT involvement by means of 97%. Should the consumer preference, management of the cloud services can be turned into partially or completely to the integrator as well.

#### 1.1.4 System reliability

Storing all records on web site can be quite risky task: Unless the person has robust safeguards in place, a energy surge or network failure can impact service operation or result in the destruction of that data. Cloud-based access control systems usually utilize centralized data centers that are formalized with efficient backup energy and storage systems to ensure the safety and integrity of the cloud service and information.

#### 1.1.5 Round-the-clock updates and monitoring

Software updates and patches are critical for ensuring that the access control system is updated and that any vulnerability is addressed. However, these updates are only beneficial if they are implemented in a well timed manner. With cloud based access to manage systems, updates may be pushed out quick and simultaneously throughout machine devices, rather than requiring employees to handle them. This helps growth device performance and security, at the same time as lowering the chance of human error. In addition, many cloud-primarily based systems offer 24/7 monitoring services, assisting enhance response time, provide peace of mind and free up stop person workforce to tackle more urgent enterprise challenges.As with traditional access control system, cloud-based solutions vary from commercial enterprise to enterprise, as do the benefits that customers care maximum about. Perhaps the most exciting gain of all is that customers can locate new methods to not only strengthen facility security, but also optimize IT and other operations commercial enterprise-wide.

### 1.2 ROLE BASED ACCESS CONTROL

The first manner a system presents protection to its sources and data, is via controlling access to the resources and the device itself. However, access control to manage is extra than just controlling which users (subjects) can get access to which computing and network sources. In addition, access control manages customers, files and different resources. It

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, May 2023

controls person's privileges to documents or sources (objects). In access manage structures numerous steps likeidentity, authentication, authorization and accountability are taken before honestly gaining access to the resources or the object in general. In early levels of computing and information technology, researchers and technologists realized the importance of preventing users from interfering every different on shared structures. Various access control systems had been developed. User's identification turned into the main index to permit users to use the system or its assets. This technique turned into known as Identification Based Access Control (IBAC). However, with the growth of the networks and the range of users, IBAC became found to be vulnerable to guard one of these large increases. Advanced ideas in access control have been brought which covered proprietor/ group/ public. IBAC proved to be problematic for dispensed structures as properly. Managing access to the device and sources has become difficult and susceptible to mistakes. A new method called Role Based Access Control (RBAC) changed into introduced. Role primarily based Access Control (RBAC) determines user's access to the system based at the role. The position a person is assigned to be basically based at the least privilege concept. The function is defined with the least amount of permissions or functionalities that is important for the job to be finished. Permissions can be provided or deleted if the privileges for a position exchange. However, issues became obvious when RBAC changed into extended across administrative domains. And it proved difficult to attain an agreement on what privileges to associate with a role.

## II. RELATED WORK

**Zhang, et al.**implemwnt the blockchain to record the interactions among users, service providers, and organizers in data auditing process as evidence, but also employ the smart contract to detect service dispute, so as to enforce the untrusted organizer to honestly identify malicious service providers. Before outsourcing data to CSPs, U and CSPs jointly generate HVT of data. Both parties confirm that their HVT is consistent with the help of blockchain. During the data auditing process, U generates a challenge nonce and requires CSPs to respond. After all CSPs calculate the respond based on challenged data blocks, O will aggregate the results into one integrity proof and send it to U through the blockchain for audit. When there is a data integrity dispute, the smart contract can judge whether the dispute exists based on the records on the blockchain, thereby preventing the framing behavior of malicious U. If the smart contract determines that there is a problem with the service provider side, it will ask O to find the malicious CSP within the specified time; otherwise it will consider O to be malicious. A prototype system is established to demonstrate that the proposed data auditing scheme is effective in a multi-cloud environment and has affordable overhead for every entity.

**Rajput,et al.** present a healthcare management framework that employs blockchain technology to provide a tamper protection application by considering safe policies. These policies involve identifying extensible access control, auditing, and tamper resistance in an emergency scenario. Blockchain is a technology to achieve a valid, challenging to tamper ledger over shared servers. Because of the blockchain network-based system's capability, when the transaction is endorsed, then the transaction is arduous to alter validly. It utilizes several consensus algorithms to reach approval on the new event for the blockchain. In general, blockchain considers the security as mentioned earlier policies to ensure the reliability of generated records, containing events, termed as blocks. Besides, it empowers authoritative participant's entry and access control and needs to support accountability. Auditing is the significant property of the blockchain. When the transaction is performed, the current block records the transaction with a timestamp, and the participant of the system trails the previous event actions. It records a history of all transactions. This strategy is beneficial for individual persons or medical organizations that require obtaining tamper-proof account records. Proposed mechanism's access rules essentially concentrate on the purpose, what data object, and which activities they have to perform. In our framework, patient predefined access permissions rules such as read, write, update, delete, and period to share their PHR by smart contracts on the blockchain without the lack of control. Smart contracts can be executed on the blockchain network once all the conditions are met.

**Li, Jiaxinget al.** develop a novel public auditing scheme for verifying data integrity in cloud storage. In the proposed scheme, different from the existing works that involve three participatory entities, only two predefined entities (i.e. data owner and cloud service provider) who may not trust each other are involved, and the third party auditor for data auditing is removed. Specifically, data owners store the lightweight verification tags on the blockchain and generate a proof by constructing the Merkle Hash Tree using the hash tags to reduce the overhead of computation and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, May 2023

communication for integrity verification. The DO outsources its data to the cloud and retrieves them when necessary. Between the DO and the CSP, the data flow should be secure and encrypted as both of them distrust each other.

The TPA, delegated by the DOs, is responsible for auditing on behalf of the DOs. Typically, a TPA centralizes the information of many DOs and provides auditing services for them. When a DO needs to verify a particular data file in the cloud, it delegates an auditing task to the TPA. Once receiving the auditing request, the TPA sends a challenge to the CSP, i.e., the TPA asks the CSP for a storage proof of the specified data file in the cloud. Then the TPA checks the responded proof and finally returns the auditing report to the DO. Typically, the challenge procedure of the auditing scheme works in the following way: A DO generates an auditing request regarding to the specified data blocks it wants to verify, and sends the request to the TPA. After receiving the request, the TPA generates a challenge with respect to the specified data blocks and sends the challenge to the CSP. When the CSP receives the challenge, it performs cryptographic operations on the verified data blocks, generates a cryptographic proof and sends the proof to the TPA. After receiving the proof, the TPA check whether the proof is correct, and sends a result to the DO.

**Shenet al.** propose proxy re-encryption and oblivious random access memory (ORAM), a privacy-preserving and untraceable scheme to support multiple users in sharing data in cloud computing. The ciphertext obtained according to the proxy re-encryption phase enables group members to implement access control and store data, thereby completing secure data sharing. On the other hand, this paper realizes data untraceability and a hidden data access pattern through a one-way circular linked table in a binary tree (OCLT) and obfuscation operation. Additionally, based on the designed structure and pointer tuple, malicious users are identified and data tampering is prevented. Based on key exchange, the proposed approach can efficiently generate the user's conference key, which can be used to protect the security of shared data and prevent malicious user collusion with other users. In addition, security of shared group data in the cloud and access control is achieved with respect to the proxy re-encryption technique. Moreover, according to the operation algorithms and the novel OCLT storage structure, our OCLT-ORAM protocol can support untraceability of address sequences and efficiency in data storage. Fault-tolerant and tamper protection features are accomplished with respect to pointer tuples. The sufficient security proof indicates the security of our protocol. The experimental comparison results could be considered as validation of the performance of our protocol, making it substantially more convincing.

**Li, Yannanet al.** propose a key updating and authenticator-evolving mechanism with zero-knowledge privacy of the stored files for secure cloud data auditing, which incorporates zero knowledge proof systems, 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, work out a re-signing key with the new private key and upload the new file tag together with some verification information to the cloud server, in which the user undertakes the least amount of the workload in the updating phase. This approach dramatically reduces the communication and computation cost while maintaining the desirable security. Each entity has his own obligations and benefits. The cloud server may be self-interested, and for his own benefits, such as to maintain its reputation, the server might even decide to hide data corruption incidents to others. Moreover, in the current time period, the cloud server can obtain the data owner's secret key in previous time periods. However, we assume that the cloud server has no incentives to reveal the hosted data to TPA because of regulations and financial incentives. TPA is responsible for checking the integrity of the cloud data on behalf the cloud users in case that they have no time, resources or feasibility to monitor their data, and returns the auditing report to the cloud user. In an auditing scheme with zero knowledge privacy, the TPA cannot learn any information of the stored data during the auditing process.

## III. EXISTING METHODOLOGIES

Cloud computing is one of the major cross-functional fields and helping many other domains to solve their problems. Health Care is one of them. Now a day Role based access control (RBAC) systems are getting more and more importance as we are more concerned about the permissions and securities attached with different role and people working in large work environment. Health Care is one of the major areas where this can be directly applicable. It provides the interesting problem of accessing people and information located at geographically dispersed locations. Many roles like Doctor, Patients and Nurse are involved in many operations ranging from creating patient record, viewing patient record and many more patient and doctor related functions.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, May 2023

### 3.1 VARIOUS ACCESS CONTROL METHODS

**1. Mandatory access control (MAC)**:

Mandatory Access Control is most commonly utilized in companies that require a multiplied emphasis at the confidentiality and class of statistics (ie. military institutions). MAC doesn't permit owners to have a say in the entities having access to in a unit or facility, rather, the data owner and custodian have the management of the access to controls. MAC will usually classify all end users and offer them with labels which allow them to benefit access to through protection with installed protection pointers.

A security model wherein access rights are regulated by way of a central authority based on a multiple levels of safety. Often utilized in authorities and army environments, classifications are assigned to device resources and the working machine or security kernel, grants or denies access to the ones resource service based at the records safety clearance of the user or device. For instance, Security Enhanced Linux is an implementation of MAC at the Linux running system.

**2. Discretionary access control (DAC):**

Discretionary Access Control is a one type of access permission system that holds the business enterprise proprietor responsible for deciding which humans are allowed in a selected location, physically or digitally. DAC is the least restrictive in comparison to the other structures, as it essentially lets in an character entire manage over any items they own, as well as the applications associated with those objects. The drawback to Discretionary Access Control is the truth that it gives the end user whole control to set security settings for different users and the permissions given to the end user are inherited into other applications they use which can probably cause malware being accomplished without the end user being aware of it.An access control method, wherein owners or administrators of the system, set the policies defining who or what's authorized to access to the resource or data. Many of these structures permit directors to restriction the propagation of access rights. A commonplace complaint of DAC systems is a lack of centralized manipulate.

**3. Role-based access control (RBAC):**

A widely used access control mechanism that restricts access to computer assets based on people or organizations with defined business functions -- executive level, engineer level 1 -- instead of the identities of individual customers. The position-based security model relies on a complicated structure of function assignments, position authorizations and function permissions developed the use of position engineering to adjust employee access to structures. RBAC systems may be used to enforce MAC and DAC frameworks.

**4. Rule-based access control:**

A security model wherein the system owner defines the rules that to manipulate access to services. Often those policies are primarily based on conditions, consisting of time of day or location based service. It is not uncommon to use some shape of both rule-primarily based access manage and role-based access control to put into effect access policies and strategies.

**5. Attribute-based access control (ABAC):**

Attribute Based Access Control (ABAC) makes use of attributes as building blocks in a structural language that defines get access to control policies and describes access requests. Attributes are sets of labels or properties that may be used to explain all of the entities that have to be taken into consideration for authorization purposes.

A technique that manages access permissions by way of evaluating a set of guidelines, regulations and relationships the use of the attributes of customers, systems and environmental conditions.

**Role based access control with user revocation and data auditing in cloud**

A new method known as Role Based Access Control (RBAC) was introduced. Role based Access Control (RBAC) determines user's access to the system based on the Job role. The role a user is assigned to be basically based on the least privilege concept. The role is defined with the least amount of permissions or functionalities that is necessary for the job to be done. Permissions can be added or deleted if the privileges for a role change. However, problems became apparent when RBAC was extended across administrative domains.

The data owner can specify a group of users that are approved to view his or her data. Any time the member of the group must access the data without the data owner's interference. Only data owner and the members of the group should access the data, no other can access the data including the Cloud Service Provider. The role-based security

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, May 2023

model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. The data owner gets back the permission to access data for any member of the group. The data owner can add new user to the group. The member of the group must not be allowed to revoke rights of other members of the group or add new users to the group. The data owner has to specify who has read/write permissions on the data owner's files.

A public verifier, such as a third-party auditor (TPA) providing expert data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server. When a public verifier wishes to check 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 public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge and-response protocol between a public verifier and the cloud server.

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. Proposed work focused on Secure Group Sharing in Cloud with Blockchain technology. 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. Proposed work designed decentralized blockchain based EHRs with AES encryption scheme. In their scheme, each authority is in charge of accessing data using their Role. That is to say, the different roles of the user are issued to more authority based on their roles. It is a hybrid cloud architecture comprising a private cloud which is used to store sensitive role hierarchy of the hospital and patient memberships, and a public cloud storing the encrypted data and public parameters associated with the Role based access control with encryption system. The users who wish to access the encrypted data and the data owners who wish to encrypt their data only interact with the public cloud.

The role hierarchy and user to role mappings related to the organization are maintained in the private cloud which is only accessible to the administrator of the hospital system. The administrator specifies the role hierarchy and the role managers who manage the user membership relations. Also implement secure user revocation process with key update system. When a user removed from existing group, group key gets updated is distributed to all users present in current data access pattern. Furthermore, all these approaches make it difficult to assign subsets of privileges of an administrator. Also provide time control key for enhance the access control performance. Using this control mechanism the allowed user can access data within the specific time. If time value gets finished, they want to ask request to access the data from cloud.

## IV. ALGORITHM

### 4.1 AES Encryption

The AES cipher is also known as the block cipher. No successful attack has been reported on AES. Some advantages of AES are easy to implement on 8-bit architecture processors and effective implementation on 32-bit architecture processors. In addition, all operations are simple (e.g, XOR, permutation and substitution). AES encryption is performed in multiple rounds. Each round has four main steps including sub-byte, shift row, mix column and add round key. Sub-byte is the substitution of bytes from a look-up table. Shift row is the shifting of rows per byte length. Mix column is multiplication over Galois field matrix. Finally, in the add round key step, the output matrix of mix column is XORed with the round key. The number of rounds used for encryption depends on the key size. For a 128-bit key, these four steps are applied to 9 rounds, where the 10th round does not consider the mix column step. Since all steps are recursive, decryption is the reverse of encryption.

**Algorithm Procedure**

The algorithm begins with an **Add round key** stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, May 2023

2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the **Mix Columns** stage. The first nine rounds of the decryption algorithm consist of the following:

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

Again, the tenth round simply leaves out the **Inverse Mix Columns** stage. Each of these stages will now be considered in more detail.

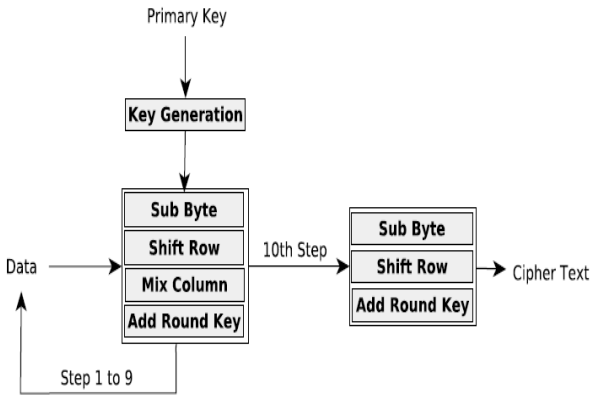


**Fig 1:** AES Algorithm for 128 bit key

### 4.2 Role Based Access Control

The Data User is provided with Role-based Access Control (RBAC) policy. In our proposed system, the privileges of the Data User are reduced and the DU can only download data from the cloud. In the proposed system, to protect the sensitive information the Data Owner specifies their own access privacy policies. Access can be restricted to certain information. Apart from this, it also helps the customer to increase his confidence and provides continuous data access with the touch of a button from anywhere at any time.

• U, R, P, and S (users, roles, permissions and sessions respectively),
• P A ⊆ P x R, a many-to-many permission to role assignment relation,
• U A ⊆ U x R, a many-to-many user to role assignment relation,
• user: $S \rightarrow U$, a function mapping each session $s_i$ to the single user user $(s_i)$ (constant for the session's lifetime), and
• roles: $S \rightarrow 2^R$, a function mapping each session $s_i$ to a set of roles $roles\ (s_i) \subseteq \{r|(user\ (s_i), r) \in UA\}$ (which can change with time) and session $s_i$ has the permissions $U_{r \in roles(s_i)}\{P|(p, r) \in PA\}$.

### 4.3 Data Access with Role Verification

1) User i constructs a sharing packet, which contains multiple secret shares $r_{ij} = r_i ID_j$ for his acquaintances, a partial public parameter $r_i Q$, and his BDID card. User i signs this sharing packet with si, $Sig_{s_i}$ (sharing packet), and then broadcasts it to other users.

2) If User j is an acquaintance of User i, User j processes the signed sharing packet as follows:

a) User j first verifies the signature $Sig_{s_i}$ (sharing packet) to ensure that the received packet is indeed originated from a user with $ID_i$.

b) User j verifies the consistence of the secret shares $r_{ij}$ with the partial public parameter $r_i Q$ through checking whether:

e($ID_j, r_i Q$,) = e($r_{ij}$, Q)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, May 2023

If the verification fails, this sharing packet is invalid, and User i is listed as a dishonest node.
c) User j checks the consistency of $ID_i$ with User i.
3) If above verifications succeed, $P_j$ accepts the secret share si j and parameter $S_i Q$.

### 4.4 User Revocation

User i picks a new random $r_i' \xrightarrow{R} Z_p$, and generates an update packet containing a new partial public parameter $r_i' Q$ and his BDID card. User i signs this packet with si, and broadcasts it other users. An acquaintance User j replaces the old partial public parameter $r_i Q$ with $r_i' Q$ after a successful verification. Thus, the new public parameter is:
$r_i' Q + r_j Q = (r_i' + r_j)Q$.

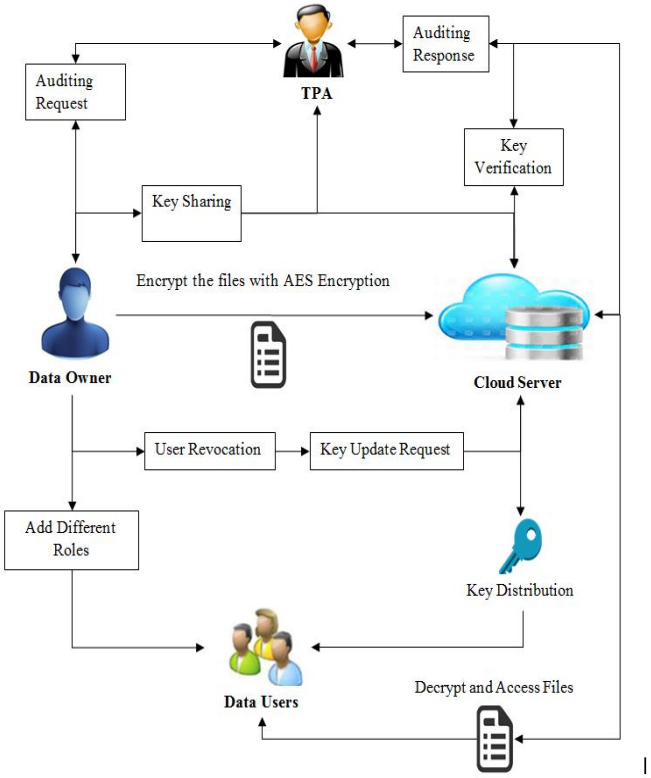


**Fig 4.1**proposed work Architecture

Here present the architecture of proposed secure cloud storage system. It is a hybrid cloud architecture comprising a private cloud which is used to store sensitive role hierarchy of the hospital and patient memberships, and a public cloud storing the encrypted data and public parameters associated with the Role based access control with encryption system. The users who wish to access the encrypted data and the data owners who wish to encrypt their data only interact with the public cloud. The role hierarchy and user to role mappings related to the organization are maintained in the private cloud which is only accessible to the administrator of the hospital system. The administrator set the role hierarchy of each user and the role managers manage the user membership relations. Also implement secure user revocation process with key update system. When a user removed from existing group, group key gets updated is distributed to all users present in current data access pattern.

## V. BENEFITS OF RBAC

- **It is solid:** Organizations can easily control users' access of information based on their roles.
- **It improves operational performance:** Thanks to RBAC many transactions are automated, and employees don't waste time using the applications and services that are not needed for fulfilling their responsibilities.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 4, May 2023

- **It decreases a risk of security breaches and data leakage**: because only a few people within an organization have access to sensitive data.
- **Scalability:**As a company grows and more employees are hired, the number of roles does not necessarily have to change. This makes it easier for the HR and IT departments, which otherwise would need to perform a number of administrative tasks.
- **Better security compliance:** RBAC implemented means that aorganization satisfies the requirements as far as privacy and confidentiality are concerned.

## VI. 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. Proposed work also supports to provide efficient integrity auditing of shared data, user revocation and supports batch auditing. TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.

## REFERENCES

[1] 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.
[2] Rajput, Ahmed Raza, Qianmu Li, and MiladTalebyAhvanooey. "A blockchain-based secret-data sharing framework for personal health records in emergency condition." In Healthcare, vol. 9, no. 2, p. 206.MDPI, 2021.
[3] Li, Jiaxing, Jigang Wu, Guiyuan Jiang, and ThambipillaiSrikanthan. "Blockchain-based public auditing for big data in cloud storage." Information Processing & Management 57, no. 6 (2020): 102382.
[4] Shen, Jian, Huijie Yang, PandiVijayakumar, and Neeraj Kumar. "A privacy-preserving and untraceable group data sharing scheme in cloud computing." IEEE Transactions on Dependable and Secure Computing 19, no. 4 (2021): 2198-2210.
[5] Li, Yannan, Yong Yu, Bo Yang, Geyong Min, and Huai Wu. "Privacy preserving cloud data auditing with efficient key update." Future Generation Computer Systems 78 (2018): 789-798.
[6] Shen, Jian, Jun Shen, Xiaofeng Chen, Xinyi Huang, and Willy Susilo. "An efficient public auditing protocol with novel dynamic structure for cloud data." IEEE Transactions on Information Forensics and Security 12, no. 10 (2017): 2402-2415.
[7] Yu, Yong, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min. "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage." IEEE Transactions on Information Forensics and Security 12, no. 4 (2016): 767-778.
[8] Shen, Wenting, Jia Yu, Hui Xia, Hanlin Zhang, Xiuqing Lu, and RongHao. "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.
[9] Shen, Wenting, Guangyang Yang, Jia Yu, Hanlin Zhang, Fanyu Kong, and RongHao. "Remote data possession checking with privacy-preserving authenticators for cloud storage." Future Generation Computer Systems 76 (2017): 136-145.
[10] Tian, Hui, Fulin Nan, Hong Jiang, Chin-Chen Chang, Jianting Ning, and Yongfeng Huang. "Public auditing for shared cloud data with efficient and secure group management." Information Sciences 472 (2019): 107-125.