Effectiveness of a Quorum Model towards Reliable Sharing of Data over Classical Models

Smita Athanere Parte 1* , Ankur Ratmele, Dr. Ritesh Dhanare, Dr. Ramesh Thakur 2

1 Computer Engineering and Science, MITS, Gwalior, MP
2 SVKM's NMIMS, Indore, MP
3 SVKM's NMIMS MPSTME Shirpur Campus, Indore, MP
4 International Institute of Professional Studies, DAVV, Indore, MP

Abstract. In recent years, cloud platforms are growing more and more popular mainly because of their outsourcing capabilities. Because cloud technology can handle massive volumes of data, many public and commercial companies are captivated by it. Moreover, cloud services provide safe data transfers between authorized and registered users. Cloud-dependent data transfer has security and privacy problems depending on how sensitive the data is. This presents a significant obstacle for cloud-based data exchange. Some of the disadvantages of the available solutions include single point of failure, difficult and inefficient data models, and user revocation. We have proposed a quorum-based. The suggested approach integrates the quorum concept with the Multi-Authority access monitoring model. Experiments for quorum and non-quorum techniques are conducted. Therefore, experimental study demonstrated that the suggested techniques are significantly more effective in terms of processing needs, memory needed, encryption decryption, and key generation. These programs are effective as well as safe from any risks to user privacy and data.

Keywords: Quorum, Cryptography, Cloud storage, Multi-authority, Access control, Group key management.

1 Introduction

With the use of virtualization and containerization technologies, on-demand computational resources are shared across the Internet with resource-constrained users; however, additional security and privacy are required. The use of cloud computing storage services has grown in prevalence over more conventional means of data storage. In recent years, an extensive range of cloud service providers have emerged, including Google Drive, Amazon S3, Azure, and Aslan (2004) and Cao et al. (2006).Data recovery and quick access are now feasible from any location at any time thanks to cloud computing technology. The use of cloud storage services has become more common for a number of reasons: (i) the availability of devices that generate enormous volumes of data, which requires a back end to store; (ii) the ease with which data can be shared with remote users; (iii) by renting storage, it lessens the overload that results from self-storage servers; (iv) it also lowers the cost of acquiring storage and maintaining all infrastructure. Even though the cloud has many services and associated advantages, there are a number of security problems and difficulties. When sharing and storing data in the cloud, these problems and obstacles call for careful consideration and handling. Since data owners must access and share their sensitive and private information, cloud servers are not completely trustworthy when it comes to access and storage. For this reason, creating access control is a crucial and challenging task. For data stored in the cloud, the access policy must be established and managed by the data owners. As seen in Figure 1, for instance, a typical enterprise scenario is provided, mentioning the hierarchical structures of all individuals within that firm. Enterprise managers have access to all of the organization's data at level 0. Research and development (R&D) managers have permitted access to all subordinates as well as their groups. Departmental engineers only have access to their own data at level 2.

A variety of encryption methods are created using access control and attribute restrictions as a basis. In this study, we

recognized and examined the problems of single points of failure and associated attacks, as well as congestion or overload on particular points of the system. Thus, a multi-authority access control system utilizing a quorum-based and non-quorum approach was proposed. By sharing computing duties among several authorities, this idea reduces the workload of centralized authority and offers effective and safe access control. With this approach, we primarily addressed three main security concerns: (i) Creating a methodical key handling mechanism to allow access to only authorized users; (ii) Encouraging safe file uploads and downloads from the cloud and data sharing among group members; and (iii) Decentralizing task distribution among various domain authorities to prevent single points of failure during group communication and data sharing.

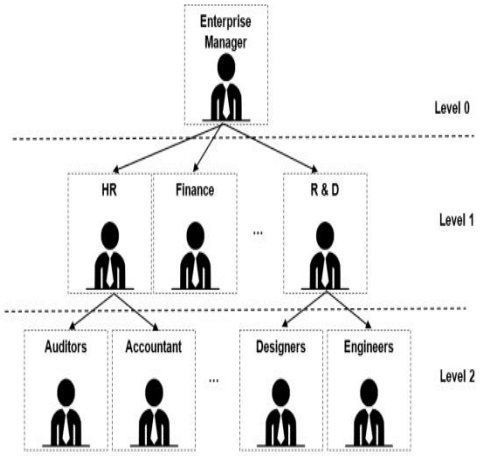


Figure 1. Organizational Access Control in Hierarchy

1.1 Motivation

Research on the current encryption methods and access control regulations has contributed to the understanding of a number of security-related problems and threats. However, the current approach adds to the burden on the centralized authority and fails to account for system dynamics such as the addition or removal of members. Therefore, designing a quorum and non-quorum based hierarchical multi-authority access control scheme for cloud environments is our primary issue (Lang et al.)[3]. It must be secure and effective. The central authority's function is eliminated in the suggested system, which also continuously monitors the dynamic behavior of cloud users. Section 1.1 presents a comparative analysis of the suggested systems based on the approaches taken, including pairing free, decentralization, attribute revocation, and multi-authority access structures.

1.1. a Comparison of proposed Scheme with Existing Work

This section covers all currently in use plans and strategies for safe data exchange. Every scheme is compared based on whether pairing is employed or not, whether there are multiple authorities or just one, the type of access structure used, whether a centralized or decentralized approach is taken, and finally, whether characteristics are revoked. It is stated in detail in Table below.

Table 1: Comparison table of Exiting schemes with proposed schemes

Method Used Decentralized	*Multi-authority Status*	*Pairing free*	*Revocation of Attributes*	*Access structure Used*	*Approaches*
Yes	*Yes*	*No*	*Yes*	*Tree*	***Chase et al.'s Approach***
Yes	*No*	*Yes*	*Yes*	*Linear secret sharing schemes*	***Ding et al.'s Approach***
Yes	*Yes*	*Yes*	*Yes*	*Tree*	***Wang et al.'s Approach***
Yes	*Yes*	*No*	*Yes*	*Linear secret sharing schemes*	***Zhang et al.'s Approach***
Yes	*Yes*	*No*	*No*	*Threshold policy*	***Xu et al.'s Approach***
Yes	*Yes*	*No*	*No*	*Linear secret sharing schemes*	***Belguith et al.'s Approach***
Yes	*Yes*	*No*	*Yes*	*Linear secret sharing schemes*	***Sethi et al.'s Approach***
Yes	*Yes*	*No*	*Yes*	*Linear secret sharing schemes*	***Ruj et al.'s Approach***
Yes	*Yes*	*No*	*Yes*	*Linear secret sharing schemes*	***Yang et al.'s Approach***
Yes	*Yes*	*No*	*Yes*	*Tree*	***Li et al.'s Approach***
Yes	*Yes*	*No*	*Yes*	*Linear secret sharing schemes*	***Liu et al.'s Approach***
Yes	*No*	*Yes*	*Yes*	*Linear secret sharing schemes*	***Fan et al.'s Approach***
Yes	*Yes*	*No*	*No*	*Linear secret sharing schemes*	***Li et al.'s Approach***
Yes	*Yes*	*No*	*No*	*Threshold policy*	***Yang et al.'s Approach***
Yes	*Yes*	*Yes*	*Yes*	*Hierarchical*	***Multi-Authority Based Approach-1***
Yes	*Yes*	*Yes*	*Yes*	*Hierarchical*	***Quorum Based Approach***

1.2 Contribution

Two unique hierarchical multi-authority access control systems, one based on quorum and the other not, that are appropriate for cloud platforms are presented in this study. The suggested plan is also more effective and safe. This suggested approach is made up of flexible and logical algorithms that manage access control and authorization rules for safe data transfer in cloud environments. The following contributions are listed:

i) To reduce the workload and address the single point of failure problem—which has been identified as a major problem with centralized entities—decentralization and the delegation of central authority functions to multiple domain authorities are advocated.

ii) Each group member's access request is approved or denied based only on their immediate domain authority, not on the authority of the central authority.

iii) A non-quorum method for reliable and secure cryptographic functions is recommended as a plan for safe data sharing. 1.

iv) The proposed strategy also suggests using a quorum-based technique for safe and effective data transfer. Based on threat level, a concept of banned users is also proposed for a certain duration.

v) Using theoretical and experimental analyses, we calculated the overhead associated with key creation, encryption/decryption, communication, and processing. It has been demonstrated that the suggested plan outperforms existing ones.

1.3 Organization

The remainder of the document is arranged as follows: In Section 2, relevant work is discussed together with specifics of current methodologies. The suggested method and related details are covered in Section 3. Section 4 contains the experimental setting, the suggested method's quorum and non-quorum design and implementation details, as well as performance and security analyses of the outcomes. Finally, Section 5 discusses the conclusion and next steps.

2 Related Work

The existing protocols (Challal and Seba, 2005) (Bonmariage and Leduc, 2006) (Chan and Chan, 2003) for group key distribution are categorized into three main classes; (1) Centralized method: where the entire group is handled by single authority; (2) Decentralized method: where entire group is partitioned into multiple sub-groups and controlled by their respective subgroup managers; and (3) Distributed approach: where the group members are in charge for generating the key. The centralized methods are mostly based on the idea of LKH (Logical key hierarchy) protocol. In this approach, a trusted server maintains a hierarchical tree structure (Velumadhava Rao et al., 2019). The decentralized approaches divide the group of members into multiple tiny groups, each of which is overseen by an intermediate key distribution server (Chan and Chan, 2003) (Jun et al., 2006) (Harte, 2008). He et al. presented a hierarchical CP-ABE (cipher text-policy attribute-based encryption) algorithm whose access structure is based on linear secret sharing technique to accomplish fine-grained access control of many hierarchical files (He et al., 2020). They also provide a hierarchical access control mechanism based on attributes (AHAC). The data associated with that section can be decrypted when the attributes of a data visitor match a component of the access control structure. Experiments reveal that AHAC has a high level of security and performance. Furthermore, as the number of encrypted data files grows, AHAC's efficiency will become more prominent [10]. The authors proposed an idea of developing the IBE approach in resource-constrained devices. We investigate various attribute authorities in this work, considering certain relevant work such as (Lewko and Waters, 2011) (Li et al., 2018) (Jouini and Rabai, 2019) all of which mainly dealt with security issues in cloud environments. Mitrra et al. proposed an idea of Iolus framework, where the Group Security Agent (GSA) is in charge of the subgroup (Mittra, 1997) (Lopriore, 2018). To detect the malware applications in mobile phone, the researchers have proposed a technique named as Rough Dorid (Riad and Ke, 2018). Identity-Based Encryption (IBE) policies provided fine-grained access control in a rapid and straightforward manner (Sahai and Waters, 2005). The access policy is also known as Cipher text-policy attribute-based encryption (CP-ABE) if it is written in cipher text. When we use the CP-ABE to encrypt a message, only members of the group with access permissions and matching attributes can receive and decrypt the cipher text.

Bhushan and Gupta presented a network flow analysis based approach. In a multimedia cloud context, it identifies and mitigates fraud-related threats (Bhushan and Gupta, 2019). However, present access control techniques have several flaws, such as dealing with collusion attacks (Bethencourt and Sahai) (Waters, 2011). To resolve these issues, the researchers further propose some innovative solutions to prevent collusion based attacks. Some of the techniques with several attribute authorities are designed for wireless area networks. Another unique technique is Attribute-Based Encryption (ABE), which uses attributes to link with data throughout the encryption process. Data and attributes are linked by private keys in a key policy-based ABE suggested by Goyal et al. (Goyal et al., 2006) . A mechanism for access control was proposed by Nair et al. In this technique, public key cryptography is used for file control, and public key cryptography is for identification (Nair et al., 2007). Niu et al. suggested an access control system for cloud environments that allows lightweight devices to securely access resources (Niu et al., 2015). Qiu et al. introduced a new key-aggregate encryption-based hierarchical access control system that allows users to share data with any user group in cloud storage. The size of each key in the proposed method is constant and unaffected by the hierarchical user

structure's scale. The proposed technique makes key administration more convenient by eliminating the key derivation that is commonly utilized in existing hierarchical key assignment methods (Qiu et al., 2019). Li et al. presented a novel multicast key distribution technique that enables multi-level controllers to oversee a specific group. The suggested technique effectively balances controller activity, improves group key distribution reliability, and allows group members to create dynamic sessions without the usage of controllers (Li et al., 2021) (Wu and Meng, 2018) (Wu, 2020) (Lopriore, 2018).

Shen et al. presented a cloud-integrated light weight certificate less authentication protocol with anonymity. This method ensures that only the network manager has access to the user's true identity (Shen et al., 2018). Along with these various techniques, quorum based technique can also be used in the hierarchical multi-authority access system. Wu et al. used quorum based scheme in key management system for wireless sensor network (Wuu et al., 2012). Zkik et al. have devised a homomorphic encryption-based authentication and confidentiality strategy, as well as a recovery-based approach for enabling secure access for mobile users at the multi-cloud server remotely (Zkik et al., 2017).

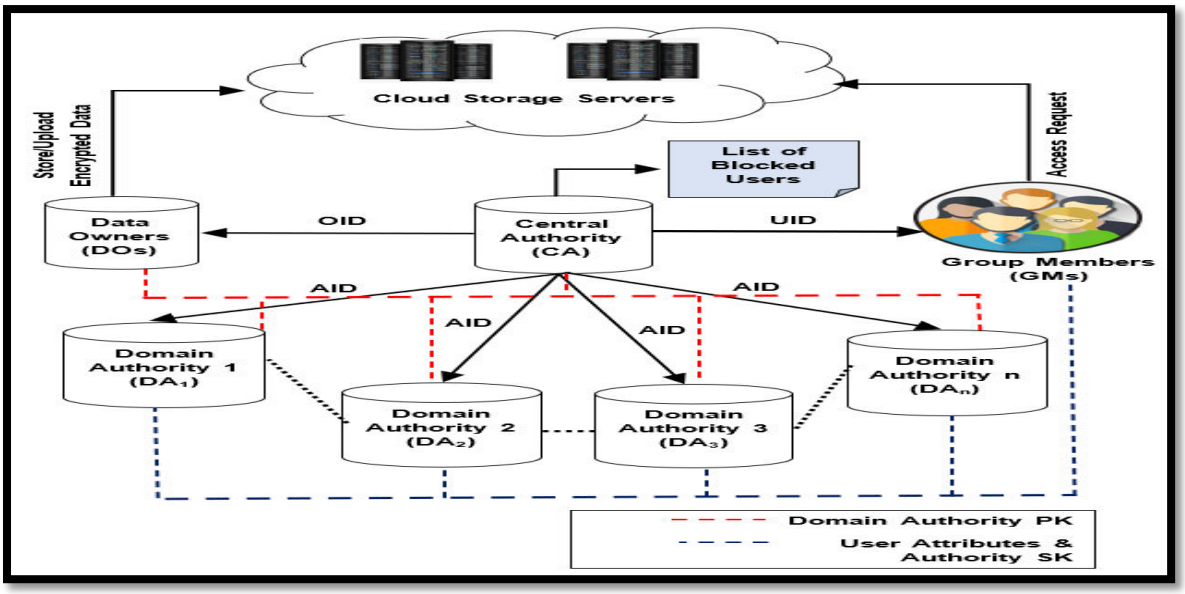
3 Proposed Work

3.1 System Model

The goal of the suggested methods, which include hierarchical multi-authority access control techniques based on quorum and non-quorum, is to transport data safely over multi-authority systems. The suggested approach involves the encryption and distribution of keys among several domain authorities. Additionally, this algorithm suggests a group of privileged users. A user's threshold level is linked to approve cloud users in order to maintain system consistency.The system model for the overall design is shown in Figure 2. Secure data sharing involves five parties: data owners (DOs), domain authorities (DAs), central authorities (CAs), and members of groups (GMs). Cloud servers are one of these parties. The following description is provided:
Storage servers on the cloud: This unit is made up of several storage servers that offer cloud services. These servers have the capacity to manage millions of requests for cloud storage and access. Only encrypted data is permitted on these servers due to security concerns. Additionally, the privacy of the data owner is preserved by these servers.

Central authority (CA): CA is responsible for managing and maintaining all DAs, DOs, and GMs. Central authorities issue unique identifiers (Uids) for each entity, such as the Owner Identifier (Oid) for data owners, the Authority Identifier (Aid) for domain authorities, and the Unique Member Identifier (Uid) for individual group members. Depending on how dangerous the network is, the CA may also put users on a blacklist for a predetermined period of time. Members can resend requests once they expire. The corresponding DA recomputed these requests.
Data owners (DOs): Owners of the data that they have put on the cloud are known as data owners, or DOs. For every file or collection of data they store on the cloud, they create their own policies. ACLs are used to store these policies. DO encrypt data before transferring it to the cloud storage platform. In a multi-authority setting, in order to get the public key of each authority, data owners must first communicate with each DA.
Domain authorities (DAx): This is a group of cloud storage servers with high processing power that can accommodate large amounts of data storage and associated access requests. The cloud storage servers do not control or have access to the data belonging to the owners. Actually, a non-privileged third-party system is what the cloud is.
Group Members (GMs): Any organization's members who wish to utilize cloud services fall into this category. These group members ask to download any firm data that DOs have stored on cloud servers. To access any file, participants must first register with the cloud and submit an access request using their [member id (Uid, File id (Fid)].

Figure 2. The proposed Quorum Based Multi-Authority System



3.2 (Quorum based Scheme):

Proposed method needs number of setups which are described as follows-

3.2. a Setup: **This section is divided into four sub-algorithms:**

CA-Setup: This setup completes the CA configuration. Various DAs receive varying amounts of Secret Si. Individual DA is also linked to a weight attribute (wa). OID is sent to DO**.**

UID Setup: In this configuration, a unique member id (UID) is produced for every member of a group. Each group member's unique user ID (UID) must be supplied in order to obtain a secret key and to upload or download data.

AID Setup: In this configuration, each DA is given a distinct domain authority (AID) by the CA. The main responsibility of AID is to protect the entire security system from unauthorized or malicious DAs that have not received validation from the CA. Additionally, each DA must choose a prime attribute, which is only used to generate the secret key for the DA as well as auxiliary keys, such as the attribute public key and secret key.

Domain Authority: Domain authority creates an attribute secret key specifically for its own collection of attributes. The members of the group use this secret key as a secret key. Attribute Public Key: Attribute driven public key generated by each domain authority**.**

Quorum forming Setup: In this configuration, the CA runs quorum formation configurations for various DAs in order to create an appropriate quorum of DAs. Quorum had to adhere to minimality and non-zero intersection properties.

.

It can be noticed that the overall responsibility of the central authority is reduced. Also, in the proposed approach, each domain authority could play the role of central authority for a set of group members.

3.2. b **Key Generation:** Every domain authority generates a pair of secret and public keys for every attribute. An distinct

AID is created in order to identify the domain authority. The public key, which is required to encrypt data, will be sent to the data owners. The members of the group will receive the secret key and use it to apply decryption. In the proposed method, we select certain public parameters, like a prime number (Y) and a randomly selected value (X).

Each member of the group is given a secret value (s), and when they join, the group as a whole chooses a random value (m). The relevant member id is applied by the authority server to construct the group key. The following equation 1 is used to represent the group key formula, or "GK.":

$$G_n = \prod_{i=1}^{l} \left\{ y + \frac{X^{s_i \oplus m_i} mod Y}{s_i \oplus m_i} \right\} + s_n \text{eq.1}$$

The secret value s_i is selected, and group members' m_i is taken in a manner such that (2<s_i< Y-2,2<m_i<Y-2). For all key operations, a randomly selected value known as the secret key, s_n, is used.

***3.2. c* Encryption:** The cipher text is the result of this step. For secure communication, the RSA Algorithm is employed. Mod y of Plaintext is Cipher text.

***3.2. d* Decryption:** Only members of the approved group are capable of decrypting the cipher text. Mod y = Ciphertext * Plaintext.

3.3 Proposed Scheme-2: (Quorum based Scheme, QHM-ACS)

3.3.1 Quorum Scheme (Request Set):

Request sets and quorum sets in our QHM-ACS can work together to achieve a key management set. According to Jiang et al. (1997), a quorum is generally defined as a request set, say R = {R1, R2,……Rn}, where each Ri is a subset of F, a universal set, given by F = {f1, f2,…….fm}. This request set, or quorum, must meet the requirements of minimality and nonempty intersection property. 50] -

- Non-empty intersection property: Any two subsets of quorum set Qs created from universal set F shall have a non-empty intersection.
- The minimum property guarantees that no subset created from universal set F can properly be a subset of another subset.

For instance, if a request set system R = {R1, R2, R3} is given, with R1 = {f1, f2}, R2 = {f2, f3}, and R3 = {f1, f3}, and a universal set F = {f1, f2, f3}, Because R's "request set" has both the minimal and non-empty intersection properties, it is regarded as a quorum system in this instance.

3.3.2 Quorum Based Hierarchical Multi-authority Access Scheme:

It's a way to guarantee that everyone has access to data from hierarchically constructed nodes. In the traditional approach, each group member can ask the central authority for permission. In the quorum-based approach, however, a group member asks the quorum—a subset of the central authority made up of domain authorities—rather than the central authority directly. This method uses three different kinds of messages: 1) Send a Request Text 2) Message in reply 3) Send Out the Word.

Request Message: To obtain permission to enter an acceptable subset of central authority, a group member sends a "request" message to every other subset of central authority in its quorum set.

Reply Message: A portion of the central authority contacts a group member in order to request permission to access the data effectively.

Release Message: To obtain the release from the subset of central authority, a subset of that authority sends a "release" message to every other group member inside its quorum set.

For effective data sharing, a quorum-based approach is used to guarantee hierarchical multi-authority access from cloud storage. The quorum determines how many failures the cluster may sustain and still be online. Quorum is designed to handle the scenario in which there is a breakdown in communication between subsets of cluster nodes, preventing multiple servers from concurrently hosting a resource group and writing to the same disc. The cluster service will be compelled to halt in one of the node subsets due to the quorum concept in order to verify that a resource group has only one legitimate owner. When a halted node is able to communicate with the main cluster of nodes once more, it will instantly rejoin the cluster and begin providing cluster services.

***3.3.3 Quorum scheme based Algorithm*:**

1. **To enter in Hierarchical System:**
   - A hub When Ni wants to access data from a hierarchical system, it sends a REQUEST message to every subset of central authority (domain authority) in the request set Ri.
   - A subset of the central authority sends a REPLY message to node Ni if it receives the request message from the node and it hasn't done so since the last RELEASE message. The request is queued if not.

2. **To access the data from hierarchical system:**
   - One element of a network is a node. Ni can access the data from the hierarchical system if it has received the REPLY message from every other domain authority server (Di) that is available in request set Ri.

3. **To release the nodes from Domain Authority:**
   - A node Ni notifies all other domain authority servers assigned to it in request set Ri of its departure from the hierarchical system by sending a RELEASE message to them.
   - When the domain authority server (Di) receives an empty queue, it modifies its status to indicate that no REPLY messages have been sent since the last RELEASE message.

3.3.4 Complexity of Messages in Quorum:

The approach requires a hierarchical multi-authority system to invoke 3√N messages per access since a request set can have up to √N members. This 3√N communication includes.

i) Complexity of request messages = √N
ii) Complexity of reply messages = √N
iii) Complexity of release messages = √N

4 Experimental Results And Analysis

4.1 Classical Method

A self-managing key management scheme with effective node-by-node authentication for networks with non-transparent relays was proposed as a solution by the researchers in a paper they published. This method works with mobile fixed and fixed things, as well as non-transparent mobile connections. It is a mixed authentication technique that includes key management along with local and distributed re-authentication. This method lengthens the relay time for stations while speeding up processing. Moreover, this method reduces not only the total overhead associated with base station and authentication server authentication. Additionally, it offers defenses against weaknesses (Khan et al., 2014) [51]. The key mechanism in this system is updated and maintained via traffic encryption key management. Because the algorithm is static, as shown in table 2, the overheads involved are constant.

4.2 Performance Analysis of Classical method and Multi Authority Quorum methods

The aspects involved at authority servers or member groups, such as key creation overhead, communication load, encryption decryption cost, and memory needs, are analyzed for the proposed approach. It is calculated according to the total number of participants in the group. Let us say the total count of group members is 'N_m'. Total members in a group can be given as 'N_m'=2^{ht}, (here 'ht' means height of member tree with $\log_2 N_{m)}$.

Table 2 presents the examination of the storage complexity at the CA server and group member, as well as the overhead of key generation and the communication between encryption and decryption. In traditional and LKH, no messages are needed during the joining and departing phase; however, in our system, due to the multi-authority idea, one message is required. Increasing the number of group members has little effect on some overheads in the traditional technique, as shown by various graphs. The DA server has a communication load during the admitting phase, however due to policies pertaining to authentication, no message is necessary for communication. LKH required more messages for encryption and decryption than the suggested approach. While LKH only employs tree structure, our approach also makes use of the notion of quorum and distinct DAs with trees. The product of attributes set of all domains calculates communication overhead as (UAT_{UID} * δ).

Figure 7 illustrates how keys are generated on the server side when a new joining is being performed. Figure 8 shows the key generation that occurs each time a group member departs. Figures 9 and 10 depict the overhead of key creation for group member nodes during the leaving and joining phases, respectively, and encryption analysis at the authority server, respectively. Furthermore, during the joining phase, Figure 11 displays encryption analysis at the group member node, and during the departing phase, Figure 12 displays decryption analysis at the authority server. Figure 14 displays storage complexity at the authority server side, while Figure 13 displays decryption analysis at the group member node during the leaving phase. The storage complexity at the group member node side is depicted in Figure 15. We have adjusted the number of authorities and bit length of items as represented in Figure 16 to examine the communication cost at the group members and DAs.

.

Scheme	Key Generation Overhead				Encryption/Decryption Overhead				Total Storage Complexity		Communi-cation Overhead
	Authority Server		Member Node of Group		Authority Server	Member Node of Group	Authority Server	Member Node of Group	Authority Server	Member Node of Group	Domain Authorities to Group Members
	Joining Phase	Leaving Phase	Joining Phase	Leaving Phase	Joining Phase	Joining Phase	Leaving Phase	Leaving Phase			
Classical	two	one	zero	zero	two	N_m-1	one	one	N_m	two	Do not support
Proposed Method	$\log_2\sqrt{N_m}$	zero	zero	one	$\log_2\sqrt{N_m}$ +1	$\log_2\sqrt{N_m}$ -1	one	zero	$2\sqrt{N}$	$\log_2\sqrt{N_m}$+ 1	$\lvert UAT_{UID}\rvert * \delta$

Table 2. Analysis of overheads among QHM-ACS, HM-ACS, LKH and classical

Execution time versus File Size of Numeric File uploads is shown in Figure 3. Execution time versus File Size of Non-numeric file upload is depicted in Figure 4. Storage in bits versus File Size of Numeric File uploads is shown in Figure 5. Storage in bits versus File Size of Non-Numeric file upload is shown in Figure 6. Decryption time versus File Size of Numeric File is shown in Figure 7.Decryption time versus File Size of Non-Numeric file is shown in Figure 7

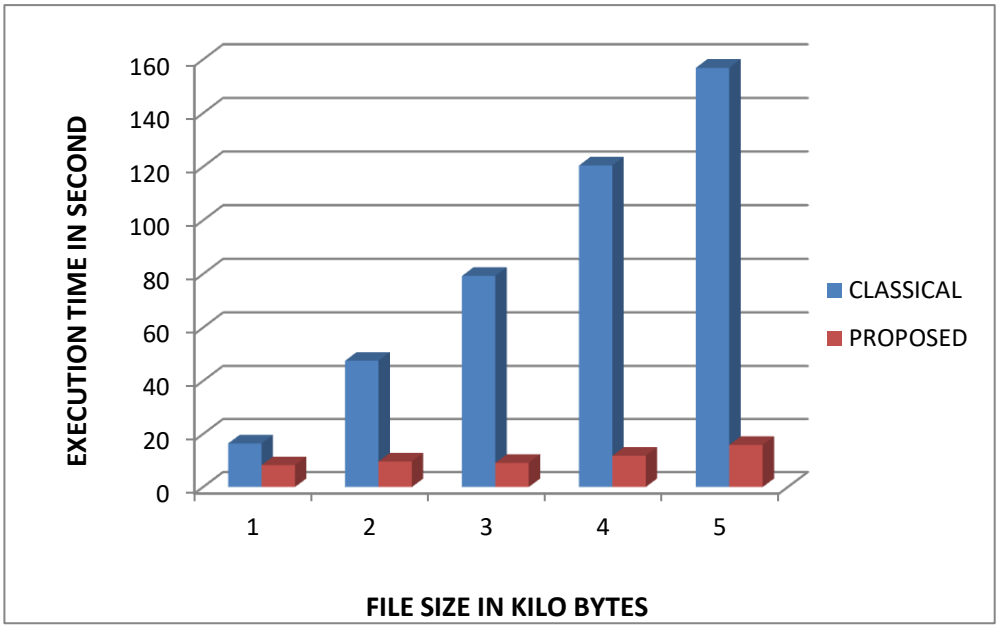


Figure3. Execution time versus File Size of Numeric File uploads

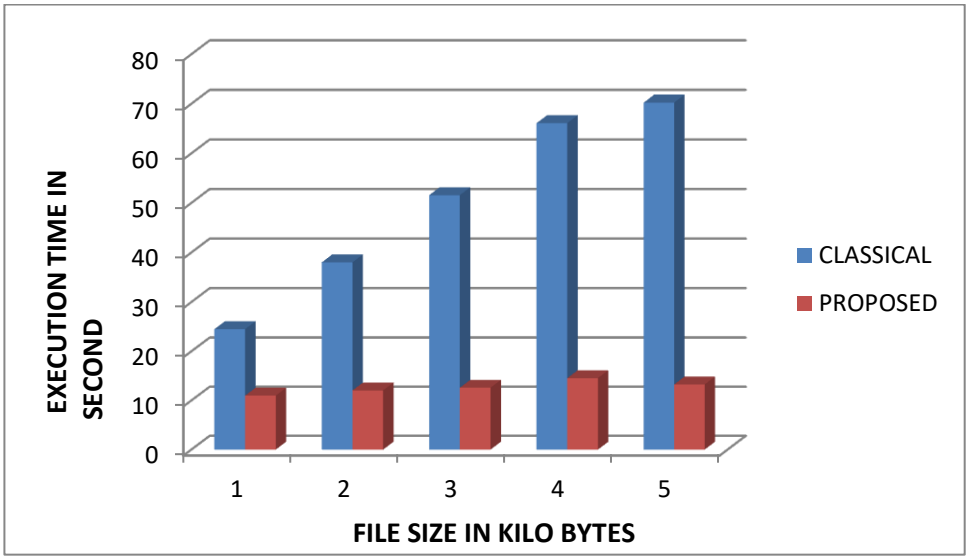


Figure 4: Execution time versus File Size of Non-numeric file upload

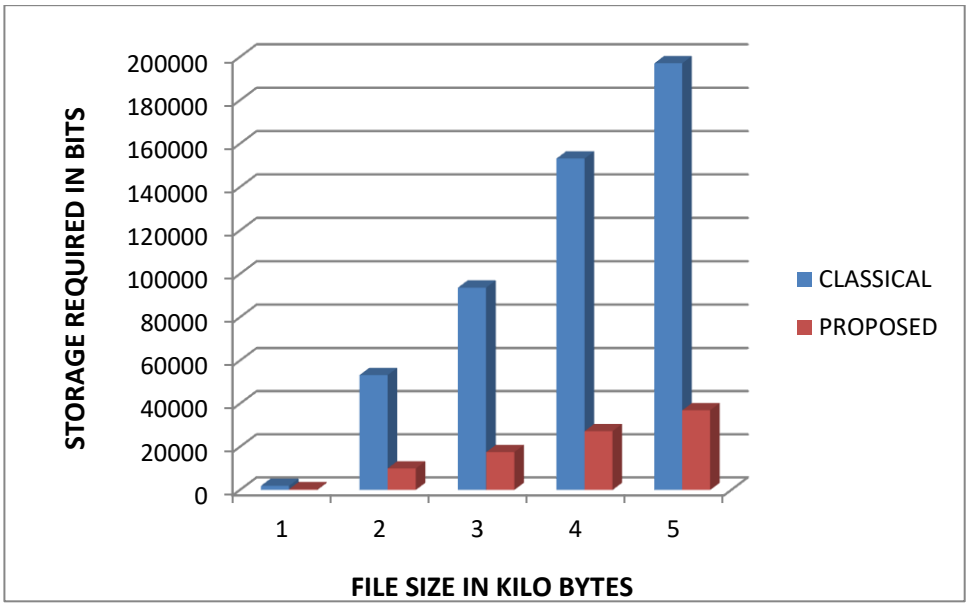


Figure 5. Storage in bits versus File Size of Numeric File uploads

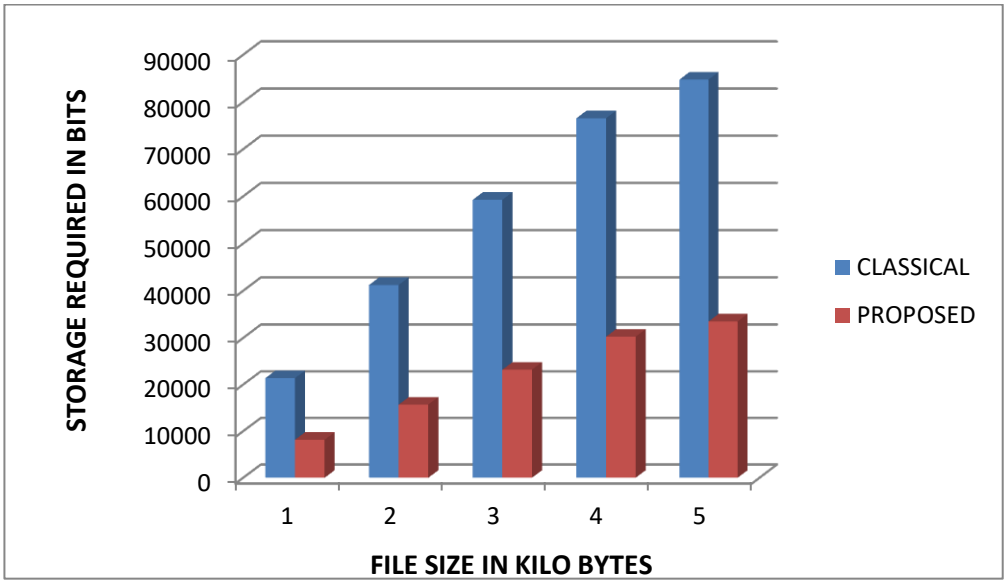


Figure 6. Storage in bits versus File Size of Non-Numeric file upload

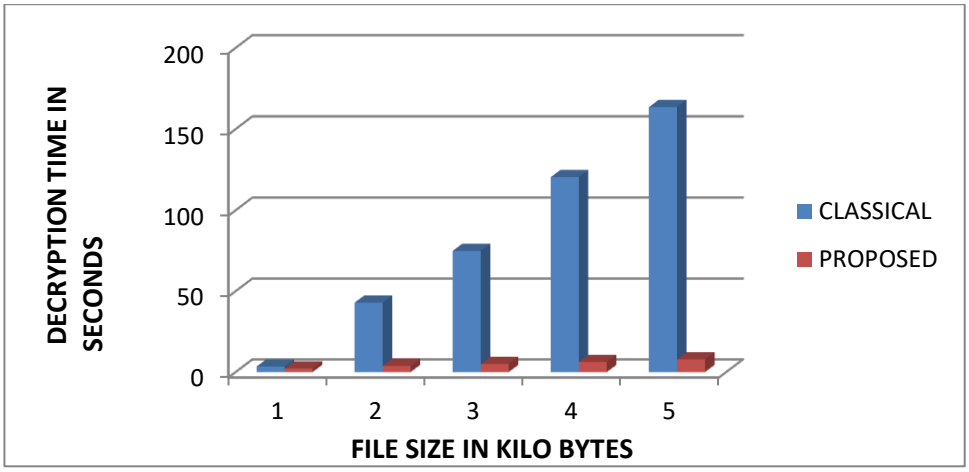


Figure 7. Decryption time versus File Size of Numeric File upload

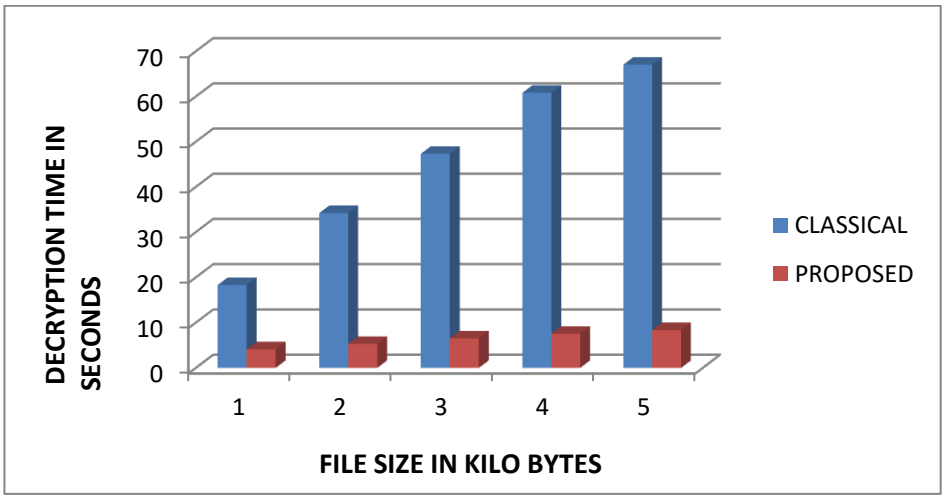


Figure 8. Decryption time versus File Size of Non-Numeric file upload

.

5 Conclusion & Future Work

In this research paper, we present an approach based on a new secure and efficient quorum based hierarchical multi-authority access control scheme for data sharing in cloud storage. The suggested framework is intended to address a variety of challenges that arise when data is shared in cloud storage. The proposed scheme achieved following key objectives. i) Task decentralization is done to avoid issue of central point of attack ii) The concept of blacklisting a specific group member is proposed in order to block the member for a predetermined length of time on the basis of current network threat level. iii) Testing findings show that the proposed schemes efficiently evaluate cloud users access requests.

The future work of proposed approach is based on linking the permission of each group member to a threshold range. This threshold range is based on the current threshold level of the group member. It can be assigned for a specific period of time and re-evaluated once the time-period is expired. In future, we can achieve a dynamic threshold-based vector to revoke the ticker for users at various stages of permission, depending on the amount of network hazard.

Conflict of Interest

We confirm that there is no conflict of interest to declare for this publication.

Acknowledgments

We would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

References

1. Aslan, H. K. 2004. A scalable and distributed multicast security protocol using a subgroup-key hierarchy. *Computers & Security,* 23, 320-329.
2. Bethencourt, J. & SAHAI, A. & Waters, B.(2007). Ciphertext-policy attribute-based encryption. 2007 IEEE Symposium on Security and Privacy (SP'07).
3. Bhushan, K. & Gupta, B. B. 2019. Network flow analysis for detection and mitigation of Fraudulent Resource Consumption (FRC) attacks in multimedia cloud computing. *Multimedia Tools and Applications,* 78, 4267-4298.
4. Bonmariage, N. & LeduC, G. 2006. A survey of optimal network congestion control for unicast and multicast transmission. *Computer networks,* 50, 448-468.
5. Cao, J., Liao, L. & Wang, G. 2006. Scalable key management for secure multicast communication in the mobile environment. *Pervasive and Mobile Computing,* 2, 187-203.
6. Challal, Y. & Seba, H. 2005. Group key management protocols: A novel taxonomy. *International journal of information technology,* 2, 105-118.
7. Chan, K.-C. & Chan, S.-H. 2003. Key management approaches to offer data confidentiality for secure multicast. *IEEE network,* 17, 30-39.
8. Goyal, V., Pandey, O., Sahai, A. & Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM conference on Computer and communications security, 2006. 89-98.
9. Harte, L. 2008. *Introduction to Data Multicasting, IP Multicast Streaming for Audio and Video Media Distribution*, Althos.
10. He, H., Zheng, L.-H., Li, P., Deng, L., Huang, L. & Chen, X. 2020. An efficient attribute-based hierarchical data access control scheme in cloud computing. *Human-centric Computing and Information Sciences,* 10, 1-19.
11. Jiang, j.-r., huang, s.-t. & kuo, y.-c. 1997. Cohorts structures for fault-tolerant k entries to a critical section. *IEEE Transactions on Computers,* 46, 222-228.
12. Jouini, M. & Rabai, L. B. A. 2019. A security framework for secure cloud computing environments. *Cloud security: Concepts, methodologies, tools, and applications.* IGI Global.

13. Jun, Z., Yu, Z., Fanyuan, M., Dawu, G. & Yingcai, B. 2006. An extension of secure group communication using key graph. *Information Sciences,* 176, 3060-3078.
14. Lang, S. & Mao, L. A torus quorum protocol for distributed mutual exclusion. Proc. of the 10th Int'l Conf. on Parallel and Distributed Computing and Systems, 1998. Citeseer, 635-638.
15. Lewko, A. & Waters, B. Decentralizing attribute-based encryption. Annual international conference on the theory and applications of cryptographic techniques, 2011. Springer, 568-588.
16. Li, J., Chen, X., Chow, S. S., Huang, Q., Wong, D. S. & Liu, Z. 2018. Multi-authority fine-grained access control with accountability and its application in cloud. *Journal of Network and Computer Applications,* 112, 89-96.
17. Lopriore, L. 2018. Key management in tree shaped hierarchies. *Information Security Journal: A Global Perspective,* 27, 205-213.
18. Mittra, S. 1997. Iolus: A framework for scalable secure multicasting. *ACM SIGCOMM Computer Communication Review,* 27, 277-288.
19. Nair, S. K., Dashti, M. T., Crispo, B. & Tanenbaum, A. S. A hybrid PKI-IBC based ephemerizer system. IFIP International Information Security Conference, 2007. Springer, 241-252.
20. Niu, S., Tu, S. & Huang, Y. 2015. An effective and secure access control system scheme in the cloud. *Chinese Journal of Electronics,* 24, 524-528.
21. Qiu, Z., Zhang, Z., Tan, S., Wang, J. & Tao, X. 2019. Hierarchical Access Control with Scalable Data Sharing in Cloud Storage. *Journal of Internet Technology,* 20, 663-676.
22. Riad, K. & Ke, L. 2018. Roughdroid: operative scheme for functional android malware detection. *Security and Communication Networks,* 2018.
23. Sahai, A. & Waters, B. Fuzzy identity-based encryption. Annual international conference on the theory and applications of cryptographic techniques, 2005. Springer, 457-473.
24. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H. & Tang, Y. 2018. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications,* 106, 117-123.
25. Toyomura, M., Kamei, S. & Kakugawa, H. A quorum-based distributed algorithm for group mutual exclusion. Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. IEEE, 742-746.
26. Velumadhava Rao, R., Selvamani, K., Kanimozhi, S. & Kannan, A. 2019. Hierarchical group key management for secure data sharing in a cloud-based environment. *Concurrency and Computation: Practice and Experience,* 31, e4866.
27. Waters, B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. International Workshop on Public Key Cryptography, 2011. Springer, 53-70.
28. Wu, Y. 2020. Developing a Taxonomic Framework of Security Methods for Security Management and Information Resource Management. *Journal of Strategic Security,* 13, 64-77.
29. Wu, Y. & Meng, F. 2018. Categorizing security for security management and information resource management. *Journal of Strategic Security,* 11, 72-84.
30. Wuu, L.-C., Hung, C.-H. & Chang, C.-M. Quorum-based key management scheme in wireless sensor networks. Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication, 2012. 1-6.
31. Zkik, K., Orhanou, G. & El HajjI, S. 2017. Secure mobile multi cloud architecture for authentication and data storage. *International Journal of Cloud Applications and Computing (IJCAC),* 7, 62-76.
32. M. Chase, "Multi-authority attribute based encryption," in Proc. of Theory of Cryptography Conference. Berlin, Heidelberg: Springer, pp. 515-534, Feb. 2007.
33. M. Chase and S. Chow, "Improving privacy and security in multi-authority10 VOLUME 4, 2016 attribute-based encryption," in *Proc. of ACM Conference on Computer and Communications Security, ACM*, NY, pp. 121-130, Jan. 2009.
34. Y. Zhang, D. Zheng, Q. Li, J. Li, and H. Li, "Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing," *Security and Communication Networks*, vol. 9, no. 16, pp.3688-3702, Aug. 2016.
35. J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE: Outsourced attribute based encryption with keyword search

function for cloud storage," *IEEE T. Ser. Computation.*, vol. 10, no. 5, pp. 715-725, Dec. 2017.
36. J. Li, X. Lin, Y. Zhang, and J. Han, "User collision avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1767-1777, Feb. 2018.
37. Q. Xu, C. Tan, W. Zhu, Y. Xiao, Z. Fan, and F. Cheng, "Decentralized attribute-based conjunctive keyword search scheme with online/offline encryption and outsource decryption for cloud computing," *Future Generation Computer Systems*, vol. 97, pp. 306-326, Mar. 2019.
38. S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT," *Computer Networks*, vol. 133, no. 14, pp. 141-156, Feb. 2018.
39. K. Sethi, A. Pradhan, and P. Bera, "Practical traceable multi-authority CPABE with outsourcing decryption and access policy updation," *Journal of Information Security and Applications*, vol. 51, pp. 102435-102450, Apr.2020.
40. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in Proc. of International Conference on Trust, *Security and Privacy in Computing and Communications*, IEEE, Liverpool, pp. 91-98, Nov. 2011.
41. K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," *IEEE T. Parall. Distr.*, vol. 26, no. 12, pp. 3461-3470, Dec. 2015.
42. Q. Li, J. Ma, R. Li, X. Liu, and J. Xiong, "Secure, efficient and revocable multi-authority access control system in cloud storage," *Computers and Security*, vol. 59, pp. 45-59, Feb. 2016.
43. Z. Liu, Z. Jiang, and X. Wang, "Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating," *Journal of Network and Computer Applications*, vol. 108, pp. 112-123, 2018.
44. S. Ding, C. Li, and H. Li, "A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT," *IEEE Access*, vol. 6, pp. 27336-27345, May. 2018.
45. Y. Wang, B. Chen, L. Li, Q. Ma, H. Li, and D. He, "Efficient and secure cipher text-policy attribute-based encryption without pairing for cloud assisted smart grid," *IEEE Access*, vol. 8, pp. 40704-40713, Feb. 2020.
46. K. Fan, T. Liu, K. Zhang, H. Li, and Y. Yang, "A secure and efficient outsourced computation on data sharing scheme for privacy computing," *Journal of Parallel and Distributed Computing*, vol. 135, pp. 169-176, Oct.2019.
47. Khan AS, Fisal N, Bakar ZA, Salawu N, Maqbool W, Ullah R, Safdar H. Secure authentication and key management protocols for mobile multihop WiMAX networks. *Indian Journal of Science and Technology*. 2014; 7(3):282–95.
48. Kei WC, Gouda M, Lam SS. Secure group communications using key graphs. *IEEE/ACM Transactions on Networking*. 2000; 8(1):16–30.