Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A HYBRID VERIFIED RE-ENCRYPTION INVOLVED PROXY SERVER TO ORGANIZE THE GROUP DYNAMICS: SHARING AND REVOCATION

P RAJA SEKHAR REDDY[1] , K RAVINDRANATH[2]

[1]Research Scholar, Koneru Lakshmaiah Education Foundation, Greenfields, Vaddeswaram, A.P., India

[2]Associate Professor ,Dept. of CSE, Koneru Lakshmaiah Education Foundation, Greenfields , Vaddeswaram,A.P.,India

E-mail: [1]prreddy.cvsr@gmail.com, [2]ravindra_ist@kluniversity.in

ABSTRACT

The Maintenance of Group Dynamics is a crucial element to any cloud service provider because of the continuous in and outflows that happen in the organizations. In group dynamics, sharing of data in encrypted format is taken care of by the attribute-based encryption (ABE), and the revocation process achieves by performing the hybrid verification procedure by the proxy server, which supports the re-encryption mechanism, which reduces the computational latency involved to double encrypt the data. The proxy server communicates with TPA to identify the malicious users or attackers. If any such users get identified immediately, the proxy server revokes the user bypassing the necessary information to the Primary Group Manager (PGM). The main advantage of the proposed system is that it performs an identity check using the primary and vital information that uniquely represents the group administrators. Also, the process involves the combination of message digest with AESWrap in a secure random key generation environment. The TPA also performs batch auditing to perform multiple audits on different groups simultaneously and increase the system's performance.

Keywords: *Group Dynamics, Re-encryption, Proxy Server, AESWrap, Secure Randomness, Revocation*

1. INTRODUCTION

The distribution of data files across the different servers is a common sharing technique that exists for decades, but there are few requirements that every data owner wants to ensure about the data /*s before outsourcing in the cloud environment, especially when a group of members accesses the same data file represents in figure 1.

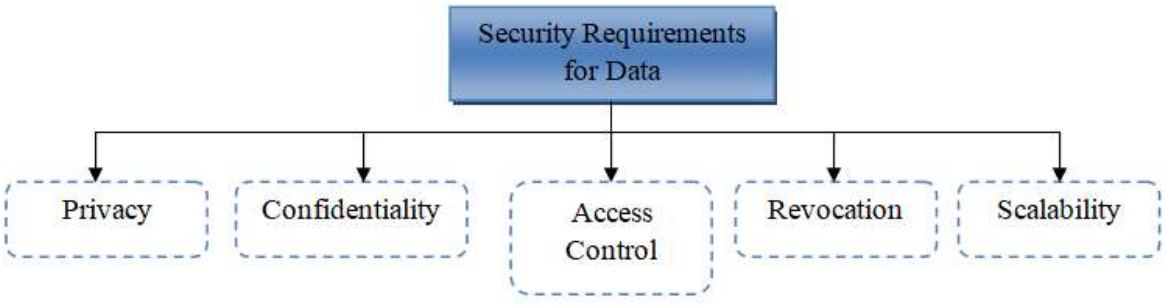

Figure 1: Security Requirements of Data Owners in case of Group Access

a. Privacy: In organizations or social media platforms, privacy is the basic concern that every user or owner expects from a cloud to protect their sensitive information from other users. The cloud has the data available in a readable format; there are many chances for either tampering with

the data in the file or hacking the resources by accessing files. Data is stored in non-readable or ciphertext format and provides only authorized access to files by exchanging the keys or granting access using the common key.

b. Confidentiality: The word confidentiality is also a protecting the sensitive data, but the key difference between privacy and confidentiality lies in "from whom the data is getting protected," like privacy deals with protecting from others users, but confidentiality deals with protecting from CSP (Cloud Service Providers). One of the main reasons for choosing the cloud environment by many organizations or users is its easy maintenance of data by clickable commands at the same it has two drawbacks; one is the data should be in the format specified by the cloud, which can make the administrator access the data and second easily is the data didn't store in a single server it may spread to different data centers then it is difficult to identify which data center is compromised or which has untrusted TPA's. So, the system needs a high-end confidentiality mechanism, which takes good measurements even to grant resources to both hardware and software.

c. Access Control: The access control issues the permissions to the different users based on authorization and grants the resources. The significant types of access control are auditing, identification, and integrity check. The access control provides policy rules to help the service features, which the users own. It also maintains and controls user profile data by restricting the other users to access unknown person's data or the user's data who don't want to share their information even with their friends. It regulates users and privileged administrative functions because the cloud act as a platform service.

d. Revocation: The revocation is a property to revoke or demolish the assigned controls to the users. Every cloud service provider has to take care of the major concern, especially while it is providing the services to IT infrastructure, where a group of users tries to access multiple files. The revocation of access control of a particular user might be due to the exit of their services from the organization, or users' attributes revokes because that particular user might be demoted from their services or user might be treated as the attacker.

e. Scalability: A cloud is efficient even if the performance doesn't degrade with the load on hardware resources. The scalability of the cloud can be achieved by providing virtual resources.

2 RELATED WORK

[1] Cloud computing provides ample resources to its users and is accessible with ease. But there may be multiple security issues like data integrity, unauthorized access to the data and data availability when the data storage is in a secluded cloud server. Data integrity is an important risk that needs to be verified whenever the problem arises. Many algorithms on auditing schemes were proposed to solve this issue, but they could not rectify the block that violates data integration. Another drawback is the accuracy in auditing for regular updating in the cloud due to the inefficient attest data structure. They designed a dynamic table where no attributes need to relocate by data modification operations to conquer this problem. The developed design can also make an auditor from the third party locate the corrupted block while data integration, thus escaping from the service denial attack and establishing a secured path for the cloud servers and mediators. The research simulation results shows that the proposed strategy costs less in computation and transmission.

[2] There are enough algorithms on the cloud to overcome the risks of data integration problems, but there are still other risks in the cloud regarding privacy issues. Some of which can be listed as information privacy acknowledgment and existence privacy, experts' misconduct of the class managers, and collusion seizure while user revocation. An auditing scheme in the cloud which uses stateless propagation for in-executive people in the dynamic class information while protecting their privacy was developed. This research also concentrated on both identity and data privacy issues by using a arbitrary masking approach. This technique accesses the t class users to track the customer's identity contributing regardless of the group managers. This eradicates the experts' misconduct of the class managers and implements non-framability. The proposed algorithm uses the concepts from Shamir secret transferring and splits the allocating process into assorted parts to avoid collusion risks. The class users can track modifications in the dynamic data from this designed binary tress and get back the updated data. They constructed an exclusive enticement using blockchain technique for data visitors and a model for transferring data to encourage the ownership to the data holder.

[3] To overcome the problem in outsourcing data in the cloud, an innovative method was designed based on the cluster–leaves – verified Merkle Hash Tree (MHT) to cluster- validate several leaf nodes and their indexes, which was very accurate only validates the several leaf nodes in sequence. The proposed dynamically auditing technique for outsourcing the data supports and protects against any corrupted attribute that leads to collusion and validates the outsourcing data by updating dynamically. The researchers say that their experimentation outcomes prove that their conclusions reduce the initialization costs for TPA and end-user. Regarding BLA-MHT, they also developed a new technique for accessing the outsourced data and dynamical updating of data. The authors claim that their experiments show the best results compared to the outdated techniques used previously.

[4] This paper explains the security threats and issues that occur to the user that access a cloud when data integrity happens, even when the TPA is involved. They say that the usage of outdated techniques and public identity key causes an issue in managing the certificate and does not encourage the dynamically updated data and tracing of user identity for class users. The TPAs used to be trusted may divert from public audit protocol or connive with server clouds for betraying users. This research solves this problem by introducing a blockchain technology that supports certificate-less multi-cloud public auditing techniques in data and multi–clones. They developed a hash-table that dynamically modifies the table's records and gains identity tracing and class user data. To prevent malignant TPA and collude to entrap users from server clouds, they used unpredictable blocks from the blockchain to develop better-confronting information.

[5] An app vendor deploys their application data on a multi-shared server through edge computing to apply to different users. Data Caching on these edge servers reduces latency in the retrieval of user's data which may lead to accidental or intentional misleading in highly – shared, volatile and dynamic computation environments. So, providing an effective audit during the cache data integration of app vendors is a vital issue to tackle. This research dealt with the Edge Data Integrity issue and introduced a simple sample dependent on a probabilistic technique named EDI – V by listing out the parameters for auditing and issue in the model to handle the integrity of data caching of app vendors on a huge scale of end servers. The sample's uniformity is managed by using a special data structure called variable – MHT or VMHT for EDI - V in establishing proof of the integrity of the replicated data while auditing.

[6] A security threat in cloud storage is affected if an abolished user and service provides of the cloud are conspired. In this research, they developed a new algorithm for data storage in the cloud that encourages modifying the data by combining unidentified revocation of class identification and vector engagement. This advanced technology enables the operation dynamically to store data by certified class users other than the data owner. If the user operates inadmissibly, the class manager can cancel his membership. A trusted TPA can audit the performance of the server cloud whenever a user modifies his data. The researchers claim that their proposed scheme encourages the changes that occur dynamically in data, and adding or leaving the class members and the data stored will not be exposed to unauthenticated users or the TPAs while data sharing and auditing.

[7] Recently, the researchers have permitted access variant cloud users to handle integrated assurance for modifications in data. Thus, it leads to substantial computational costs for the cloud users even though new techniques with greater reality were introduced. To manage public auditing in the cases of data integration, an effective and potent algorithm was developed in this research. This study used cryptography furnished with surrogate re-encryption and a hash function in cryptography. They accessed a TPA to perform the data preprocessing regarding the cloud users before transferring the data CSPs and validate the data integrity and perform data re-encryption to transfer the data in privacy. This technique is portrayed by the consequential properties like private key management, key exchanges, reducing burdens for clients, cost redundant calculations, CSPs failure for developing the apt verifier answer without data and requirement of one – time key.

[8] With advancements in cloud services technology, many cyber threats were also raising the privacy and privacy, integrity, and security concerns among the cloud platform users. These threats and unwanted addition of confidential data of customers is a relevant issue for outsourcing data. Therefore, implementing the

necessary CSPs and performing rights of data access was a better solution. To avoid further damage while implementing the Group Dynamic fields, this research develops a model that is effective in data sharing when the custodian of the program is low, protected ease in sharing of data within the cloud storage and modifications in the re-encryption keys by the community will be minimized [9-14]. This innovative model handles the user cancellation issues efficiently irrespective of the overburden of the cloud server, system admin or KAM.

3. PROPOSED METHODOLOGY

In ancient days, there is a concept known as "Broadcast," The data owner shares the encrypted key with all the users of the same group in the cloud irrespective of the authorization details. The complete evaluation process of broadcasting represents in table 1.

Table 1: Evaluation Process of Proxy Re-encryption Technique

S.No	Author Name	Mechanism	Limitation
1	Berkovits	Broadcast Encryption (BE)	Any user can easily decrypt the details of other users in their group
2	Sakai and Furukawa	Identity-based BE (IBBE)	With the public key created from the user ID, it is easy to crack the user details
3	Deliverables	Constant Size IBBE	The generated ciphertext is of fixed size, and it uses a simple substitution technique. So the chances of getting attacked are high
4	Boneh and Franklin	Time-stamped IBBE	The public key generates as a combination of user ID and time of creation. It involves many computations to incorporate time as a series
5	Green and Ateniese	Proxy Re-encryption	It doesn't have mechanisms that can revoke access control from attackers.

The proposed method deals with the problems that occur due to the sharing of data between the multiple users using the enhanced proxy server, which is implemented in the cloud and is controlled by the Primary Group Manager (PGM) and Third-party Auditor (TPA). The proposed system tries to address the problems in table x by integrating the re-encryption technique in proxy server with hybrid identity check to revoke the access controls granted to the unauthorized users, and it also shares the data in the encrypted form. These type of systems helps to avoid the multi computations that occur during the revocation process, and it provides high security even though there is no update on the key value, which is shared among the group of users when some revocation process occurs in the cloud. The proposed system entire architecture and its workflow illustrates in figure 2

Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

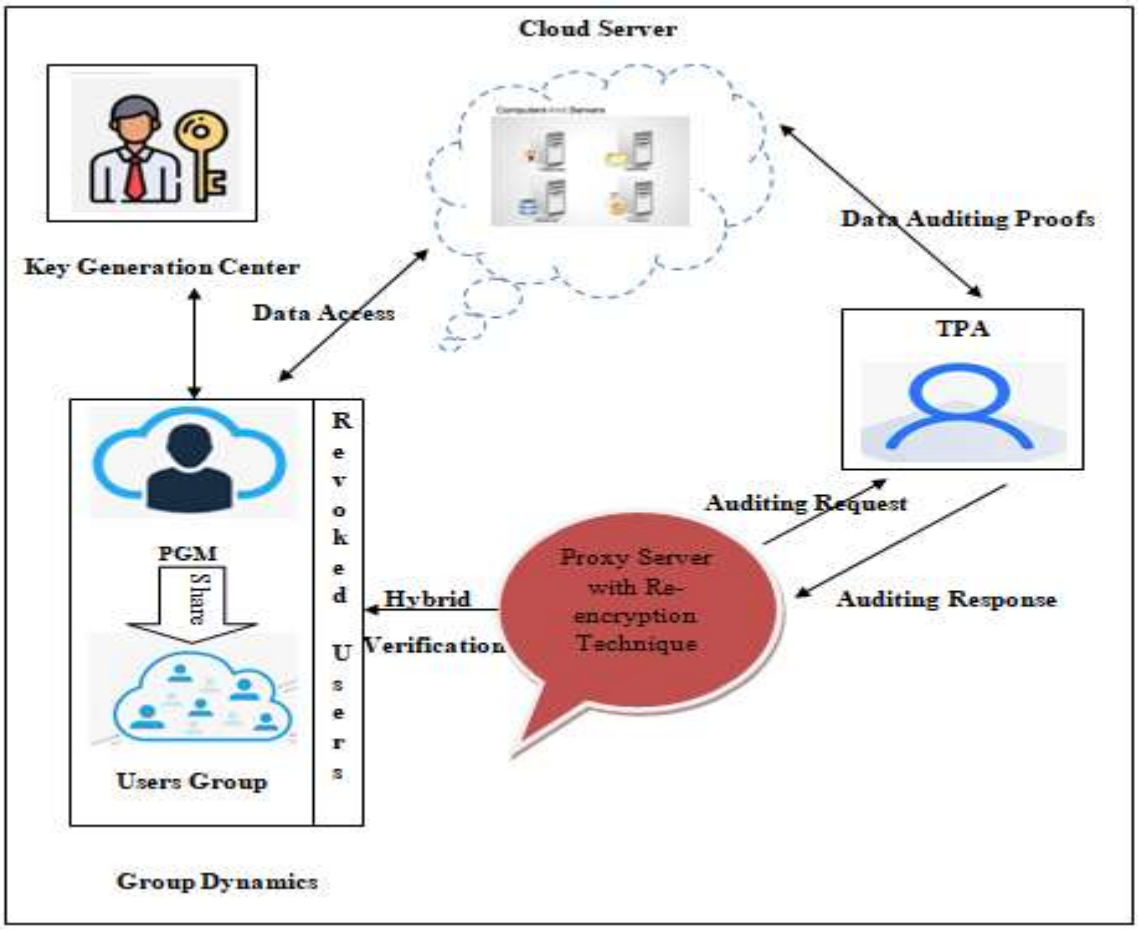

Figure 2: Architecture for Describing Work Flow in Cloud with Group Dynamics

Figure 2 states that five important modules constitute working with this group dynamics. This section of the paper describes every module in detail, including necessary pseudocodes.

3.1 Key Generation Centre: This module generates the public and private keys among the group users. The important property of scalability is achieved by exchanging the information with the help of keys generated by the KGC. In the proposed system, the generation of keys is taken care of by random pairs of keys integrated with the message digest. The nature of randomness has a great impact on the working of hardware resources like if the system implements operating system-based random functionality there are huge chances for the resources to get blocked. The proposed system keeping the properties of reliability and unpredictability in view, implemented the secure randomness extending its support with anti-patterns of different cloud properties.

Pseudocode for Random Key Generation:

1. Key_gen←prepare the instance for MD5

2. randomly initialize the key size

3. key_pair←initialize the values with a key size

4. call generate_key_pair() to produce the public key

5. broadcast the generated key with users

3.2 Cloud Server: The entire authorization responsibilities are taken care of by the cloud server, including the TPA and Proxy server, by using an integrated approach that uses a combination of AESWrap block cipher in GCM mode and message digest, which is a popular key agreement policy by hyper tuning the necessary parameters. The reason for AES to operate in GCM mode is to authenticate every block of the cipher by attaching a tag of 128-bit length. In

general, GCM mode applies padding to its data bits during the transmission, but the proposed system uses padding as a multiple of data block size, provided by the PKCS5Padding schema. The key size is customized in this system because the key length of 128 or 256 bits is strong to break, but they need more computational resources to encrypt. The DRBG mechanism is used to implement the encryption process. The second part of the algorithm deals with message digest with good hash properties, with flexible key length.

Pseudocode for Encryption:

1. k[]←generateKey().getEncoded()

2. kspec←secretKeySpec(k,"AESWrap")

3. cip_txt←getInstance("AESWrap/GCM/Padding")

4. for i←0 to data.length:

   i. part[i]←data.segment(size="s")

   ii. mdata[i]←update(part[i]).getBytes()

   iii. hash_func←mdata[i].digest()

while constructing the proposed system, the algorithm has taken few considerations as shown in table 2 into consideration

Table 2: Parameter Considerations of Proposed Algorithm

S.No	Parameter Name	Possible Values	Parameter Value
1	Mode of Operation	GCM/CCM	GCM
2	Padding Scheme	ISO10126Padding/ PKCS5Padding/ No padding	PKCS5Padding
3	Key Size	128/256 bits	Dynamic Key Size
4	Deterministic	Same size as a digest	Same size as a digest

3.3 Proxy Server: The major work of the Proxy server lies in the process of group dynamics revocation. Traditional approaches use sharing of a single encrypted key among the group users, which involves many computational overheads even if a single user exits from the group. To solve this, proxy servers with the motivation of re-encryption came into existence. The overview on the different proxy server based on their encryption mechanisms are showcased in figure 3.

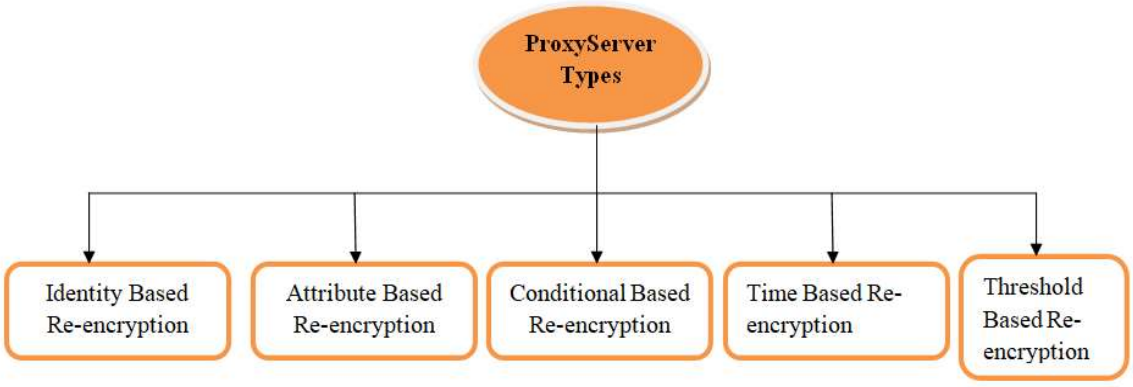

Figure 3: Classification of Proxy Servers based on Re-encryption Mechanisms

Different re-encryption techniques have different issues like collusion problems, double encryption operations with high complexities involved. The proxy server uses a hybrid verification procedure to revoke the user's permissions from time to time. The proxy server tries to provide encryption based on the user's email address attributes, generally, which is treated as a powerful unique attribute. The proxy server encrypts the details of the users based on their

email id. The main advantage of this re-encryption mechanism is that it need not rework on the plain text, but the process of generating a private key based on their identity for every individual involves more time. To handle this problem, the proposed system generates the keys based on their level of authorization by taking the identity of group admin as a security check; since few group administrators are available so its complexity reduces to produce the secret key.

Pseudocode for Hybrid Re-encryption Revocation Process

1. Public_Key_Gen←input(group admin email address)

2. broadcast(Public_Key_Gen)

3. Identity_key←encrypt(PKG)

4. proxy_server_key←receive(Identity_key)

5. re_pro_key←encrypt(proxy_server_key)

3.4 Third Party Auditor (TPA): To utilize the cloud services insecurely, an agreement called "Service Level" must be authorized at the cloud server level. So, an auditing mechanism is required to validate the agreement rules continuously. Since the proposed system has multiple users accessing the cloud, it implements a batch auditing scheme using TPA, which gives results neutral to data owners and cloud servers. The main advantage of batch processing lies in verifying and auditing multiple users simultaneously by challenging the cloud server. The major operations are: setting the environment to run the master key based on the security parameters, the user personal details are extracted and are encrypted, which can be used as the secret key, a digital signature is generated to verify the user authentication when the user wants to decrypt the documents and access them for further manipulations. Every document is marked with flags and tags to update them timely. All the audited files should be uploaded into the cloud server, so the system uses two steps while interacting with the cloud generating the proofs by marking the subsets and evaluating the cloud server's challenge and the proofs evaluated by evaluating the accuracy parameters on the validated test data. The process of TPA is illustrated in figure 4.

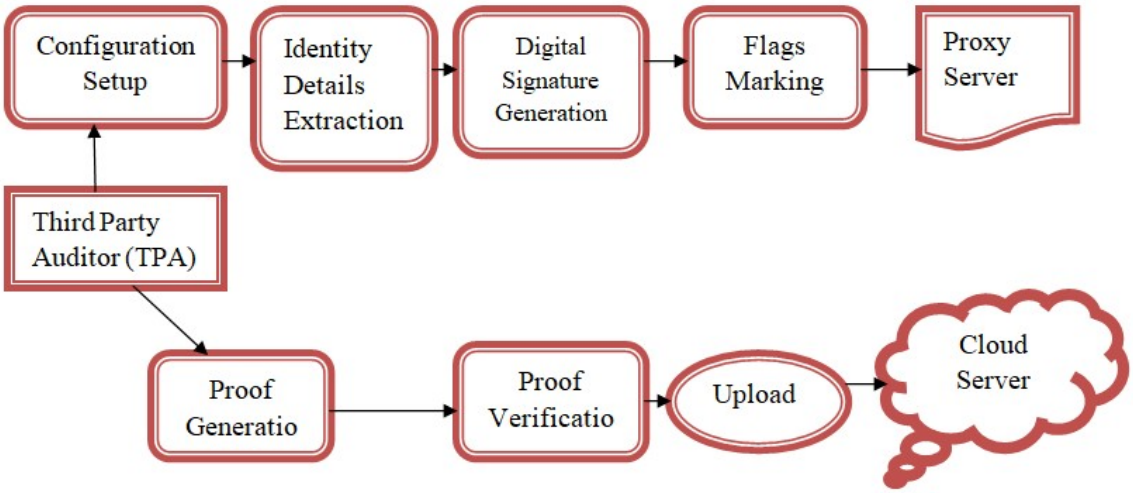

Figure 4: Communication of TPA during the process of auditing

3.5 Primary Group Manager: The Task of the PGM module protects the data from unauthorized sources by generating the signature based on the group user identities and broadcasting the obtained secret key across the group. The PGM also maintains the list of revoked users for detaching the resources allocated to the user and communicates the same with other users to provide more security.

Pseudocode for Signature Generation for Group Users:

1. Data←Input from data owners

2. for i in groups.length:

   a. r[i]←SecureRandom()

   b. generate hash_function(r[i])

3. compute the challenge using hash functions and timestamp produced by server

4. for i in groups.length:

   i. sig[i]←challenge^hash_function(r[i])

5. broadcast(sig)

4. RESULTS & DISCUSSION:

The evaluation of the cloud computing environment is discussed on various parameters as discussed in this section. The processing time required to perform different operations on the file is represented in table 3.

Table 3: Computational Times Of Different Functions In Units Of (Ms)

S.No	Uploading	Auditing	Sign Generation	Verification
[1]	0.0067	0.000093	0.0044	0.40
[2]	0.0892	0.000345	0.1036	0.435
Proposed Algorithm	0.0052	0.000007	0.0013	0.358

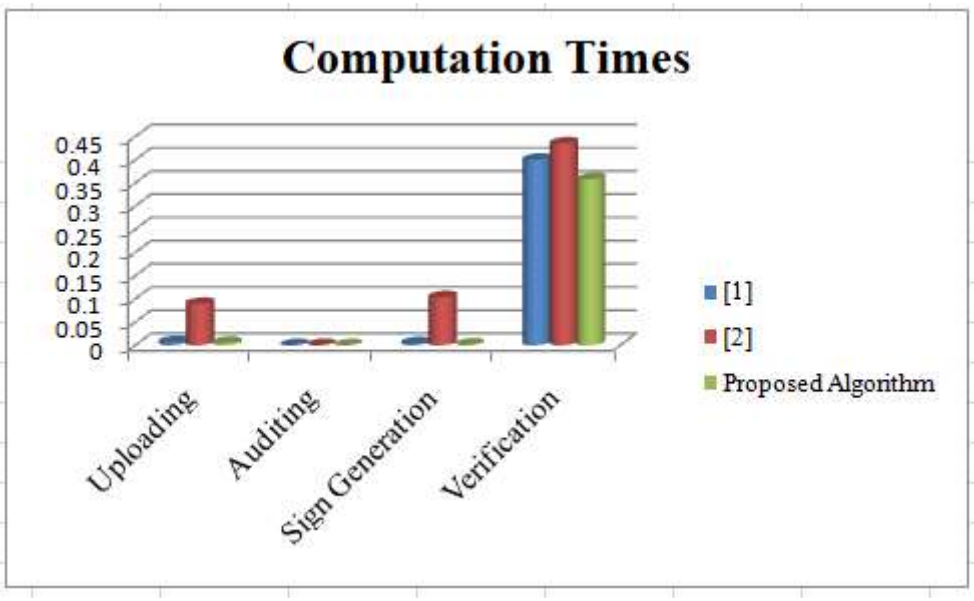

Figure 5: Analysis of Different Operations Computation Times

Figure 5 shows that the proposed algorithm needs less time to perform any sort of operations related to the cloud. Due to this complexity, more powerful algorithms which are resistant to collusion are much worse than the normal algorithm that operates on ABE. The process of data auditing is examined in two different cases by using various algorithms and is illustrated using the different algorithms as shown in table x.

Table 4: Case Study on different operations performed by TPA

S.No	Tag Generation	Data Auditing	Proof verification	Challenge
[3]	0.56	0.72	0.0088	0.49
[6]	0.60	0.72	0.076	0.498
[4]	0.6588	0.856	0.00056	0.562
Proposed Algorithm	0.342	0.0067	0.0051	0.43

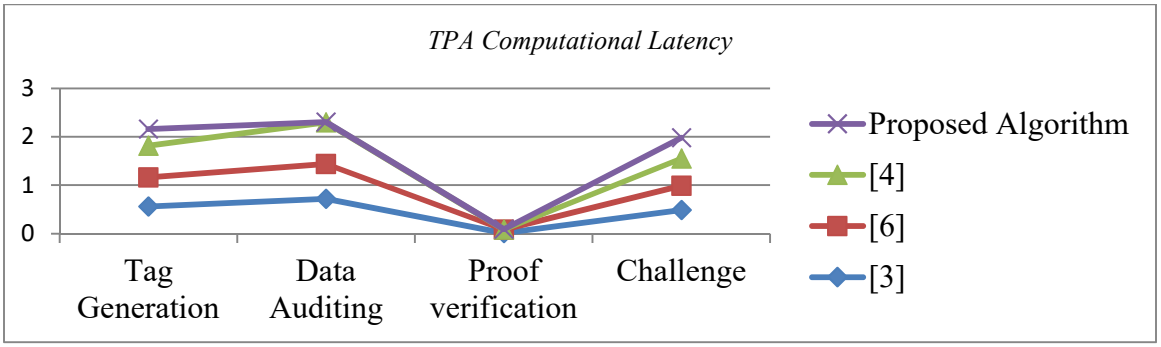

Figure 6: Computational Latency

Figure 6 determines the flaws among the previous mechanisms and proved that signature has its own implementations that really helps the user to deal with complicated issues that are involved because of certification authority.

The accessing of data gets delayed sometimes due to latency in providing the necessary resources to the user. This is illustrated in table 5.

Table 5: Delay in Accessing of files

File Name	Size in GB	Time in ns
Security	160	0.98
BlockChain	30	0.0001
Data Analytics	145	0.84

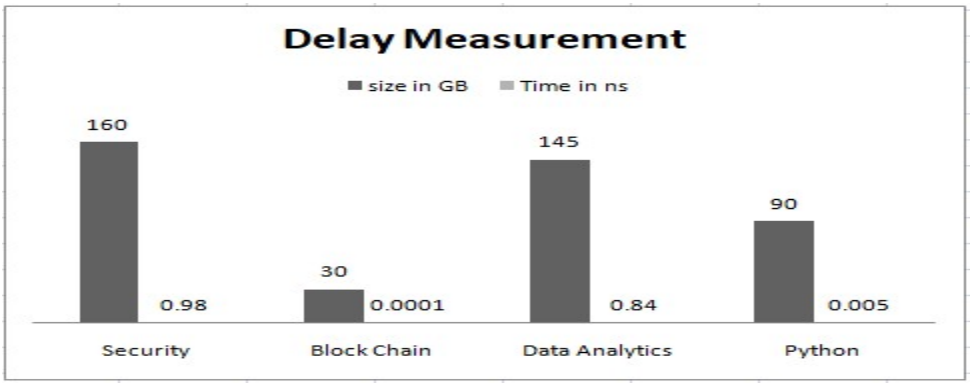

Figure 7: Time Delay in Accessing a File

Figure 7 states that with the increase in the size of data blocks, there might be some delay in accessing a file. But the throughput is efficient because the delay is very small when compared to the other systems.

5. CONCLUSION

The data auditing scheme is verified by the certification authority based on the encryption keys. The system can efficiently revoke many users even the attackers within a considerable amount of time without re-computing the private keys or updating the shared key among the groups. The combination of SLA and certification authority schemes prevents attackers or malicious users from accessing the higher-level protocol. The tags attached to the data blocks by the proxy server help the group's administrator to have some kind of confirmation about the audited data even though the TPA compromises with the cloud environment. The re-encryption mechanism has adaptive nature, which solves collusion restraint by fine-graining the access control by sharing the encrypted data among multiple users. In further work, the malicious TPAs can be identified by using efficient genetic algorithms and threshold-based encryption to increase the scalability of the systems.

REFERENCES:

[1]. Yu, H., Lu, X., & Pan, Z. (2020). An Authorized Public Auditing Scheme for Dynamic Big Data Storage in Cloud Computing. IEEE Access, 8, 151465–151473. https://doi.org/10.1109/access.2020.3016760.

[2]. Yang, X., Wang, M., Wang, X., Chen, G., & Wang, C. (2020). Stateless Cloud Auditing Scheme for Non-Manager Dynamic Group Data With Privacy Preservation. IEEE Access, 8, 212888–212903. https://doi.org/10.1109/access.2020.3039981.

[3]. Rao, L., Zhang, H., & Tu, T. (2020). Dynamic Outsourced Auditing Services for Cloud Storage Based on Batch-Leaves-Authenticated Merkle Hash Tree. IEEE Transactions on Services Computing, 13(3), 451–463. https://doi.org/10.1109/tsc.2017.2708116.

[4]. Yang, X., Pei, X., Wang, M., Li, T., & Wang, C. (2020). Multi-Replica and Multi-Cloud Data Public Audit Scheme Based on Blockchain. IEEE Access, 8, 144809–144822. https://doi.org/10.1109/access.2020.3014510.

[5]. Li, B., He, Q., Chen, F., Jin, H., Xiang, Y., & Yang, Y. (2021). Auditing Cache Data Integrity in the Edge Computing Environment. IEEE Transactions on Parallel and Distributed Systems, 32(5), 1210–1223. https://doi.org/10.1109/tpds.2020.3043755.

[6]. Zhang, Y., Chen, C., Zheng, D., Guo, R., & Xu, S. (2019). Shared Dynamic Data Audit Supporting Anonymous User Revocation in Cloud Storage. IEEE Access, 7, 113832–113843. https://doi.org/10.1109/access.2019.2935180.

[7]. Hussien, Z. A., Abduljabbar, Z. A., Hussain, M. A., Al Sibahee, M. A., Lu, S., & AL-Asadi, H. A. (2019). An Efficient and Secure Scheme for Dynamic Shared Data in Cloud. Proceedings of the 3rd International Conference on Computer Science and Application Engineering - CSAE 2019. the 3rd International Conference. https://doi.org/10.1145/3331453.3361648.

[8]. Agarwal, Prerna & Singh, Satya. (2021). A Hybrid Cryptographic System for Dynamic Cloud Groups with Secure Sharing of Data and Proficient Revocation of Users. Solid State Technology. Volume: 63 Issue: 2s.

[9]. Ayaluri MR, K. SR, Konda SR, Chidirala SR. 2021. Efficient steganalysis using convolutional auto encoder network to ensure original image quality. PeerJ Computer Science 7:e356 https://doi.org/10.7717/peerj-cs.356.

[10]. A.Mallikarjuna, B. Karuna Sree, " Security towards Flooding Attacks in Inter Domain Routing Object using Ad hoc Network" International Journal of Engineering and Advanced Technology (IJEAT), Volume-8 Issue-3, February 2019.

[11]. Chandrasekhara Reddy, T., Pranathi, P., Mallikarjun Reddy, A., Vishnu Murthy, G., Kavati,I., et al., (2019), Biometric template security using convex hulls features Journal of Computational and Theoretical Nanoscience, Volume 16, Numbers 5-6, May, pp. 1947-1950(4), doi: 10.1166/jctn.2019.7829.

[12]. Mallikarjuna Reddy, A., Rupa Kinnera, G., Chandrasekhara Reddy, T., Vishnu Murthy, G., et al., (2019), "Generating cancelable fingerprint template using triangular structures", Journal of Computational and Theoretical Nanoscience, Volume 16, Numbers 5-6, pp. 1951-1955(5), doi: https://doi.org/10.1166/jctn.2019.7830.

[13]. Dayaker, P., Honey Diana, Chandrasekhara Reddy, T., Mallikarjuna Reddyreddy, A." Advancements of security and privacy of sensitive data cloud computing" Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 11-Special Issue, 2018.

[14]. Kumar, R.A., Mallikarjuna Reddy, A., Chandrasekhar Reddy, T., Ravi Kishore, M.,"A study of block chain technology and cryptocurrency" Jour of Adv Research in Dynamical & Control Systems, pp.no 994-1000,Vol. 10, 11-Special Issue, 2018 .