International Journal of LNCT, Vol 1(1)
ISSN (Online): 2456-9895

Multi-Stage security of shared dynamic cloud data with automatic group user revocation

Madhurima Sharma[1] and Rachana Dubey [2]
M. Tech. Research Scholar , Department of Computer Science and Engineering, LNCT, Bhopal[1]
Associate Professor, Department of Computer Science and Engineering, LNCT, Bhopal[2]

Abstract
The security of the information while sharing is very necessary as it is possible to multiple users. The privacy of the content is needed to protect simultaneously maintaining the shared access to authorized users. In this work while managing the privacy as well as security if shared data some added and layers of security is proposed. The group users while accessing the shared information will be blocked on first wrong attempt and need administrator permission to get login access. Even all the data are encrypted with keys so that with wrong keys and authorization credentials no one will be able to access the shared data. These multiple layers increasing the protection of user shared data.

Keywords
Public integrity auditing, Dynamic data, Victor commitment, Group signature, Cloud computing.

1.Introduction
Cloud concept is nothing but also the storage service, but it can also share across multiple users. We generally organizes protection safeguarding system on the grounds that amid inspecting information from cloud administrations it's not a secured while that private data is freely ensured by cloud benefit. To others including new joining clients which shields the classification from the disavowed clients in the dynamic communicate encryption conspire. We suggest that when any client is getting to the information from the cloud it must be guaranteed from unapproved individual or programmer. Cloud is un-trusted record stockpiling, so we use encryption based get to control for sharing archive in the distributed storage benefit. The client's information is scrambled by utilizing cryptographic strategy from unapproved individual that can hack the client's private information. In this cryptographic strategy we utilizes distinctive calculations like mark calculation, key era calculation, ring confirm algorithm, etc. These calculations are utilized as a part of the cryptographic system. Clients can appreciate great administrations by moving nearby information administration frameworks into cloud servers. Figure 1 shows the storage model.

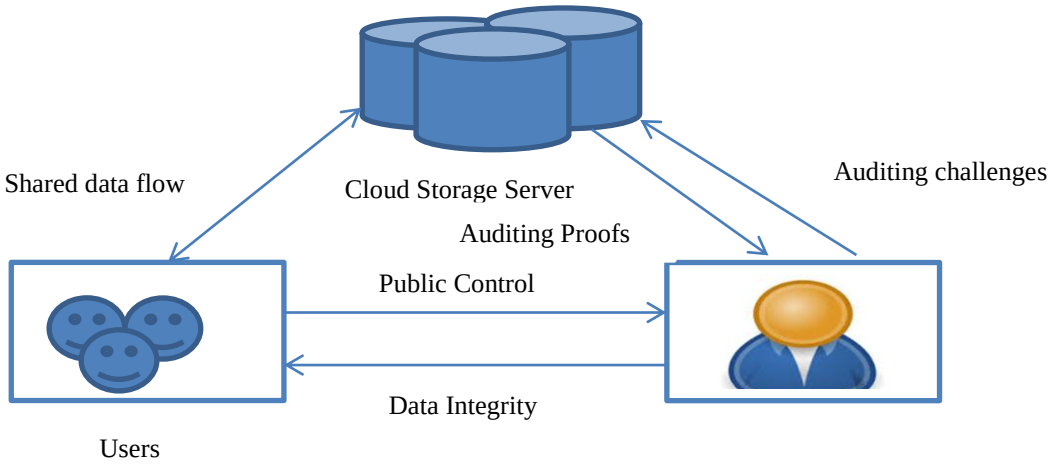

Figure 1 The cloud storage model

Real world examples are cloud based synchronization platforms such as drop box for business [1] ,online data backup services of Amazon and some practical cloud based software Google drive [2].Which enables multiple team members to work in synchronous Accessing and modifying same file on cloud servers

anywhere any time. For proper execution of this kind of cloud based collaborative applications one problem is to assure data integration i.e. each data modification operation is simply performed by an authorized member and the data remains intact thereafter. This problem is important given the fact that cloud platforms, even well-known .cloud platforms may experience hard ware software failure human errors and malicious attacks [3, 4].

Service availability, data synchronization between different devices, possibility of data via any devices which includes browser facility makes cloud more interesting. Now since the info gets shared or saved in provider's area, the client gets worried about privacy of its data, although there are certain accommodation and SLA which are agreed by cloud provider and client. Now although client has a platform to share the info, the charges of securing his/her data or in a nutshell making its data secret gets costlier.

The cloud term is of interest not due to the patient clients but to organizations as well. With organization as a consumer the concern about data security becomes multifold. Keep in mind a typical example of small scale business that has different departments like HR, Finance, etc. Therefore securing this finance data is vital before it gets uploaded to the storage cloud, and just in case the data saved in cloud storage gets tampered there should be a method to certify the integrity of the data, moving further specific band of people should have access to this data which may be folks from finance department of client company or special auditors. Simply speaking the client should have the ability to save the data securely, certify the integrity of the data, and share the data securely with specific band of people.

Cloud benefit specialists deal with an endeavour class framework that offers an adaptable, secure and dependable condition for clients, at a much decrease peripheral cost because of the sharing way of assets. Dropbox and Google Docs. The integrity of data in cloud storage, however, is a subject to skepticism and scrutiny, as data saved in an un-trusted cloud that can easily be lost or corrupted, due to hardware failing and human errors. To protect the integrity of cloud data, by perform public auditing through introducing to a third party auditor (TPA), who offers its auditing service with more powerful computation and delivery abilities than regular users.

2.Literature survey

In [1], proposed a scheme to realize efficient and secure data integrity auditing for share dynamic data with multi-user modification. The scheme vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures along with user revocation are adopt to achieve the data integrity auditing of remote data. Beside the public data auditing, the combining of the three primitive enable our scheme to outsource cipher-text database to remote cloud and support secure group users revocation to shared dynamic data.

Provable data possession (PDP), first proposed in [2], allows a verifier to check the accuracy of a client's data saved at an un-trusted server. By utilizing the RSA-based homomorphic authenticators and sampling strategies, the auditor is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public verifiability or public auditing. Unfortunately, their scheme is only suitable for auditing the integrity of static data.

In [3] defined another identical model called proofs of retrievability (POR), which is also able to check the correctness of data on an untrusted server. The main file is added with a set of randomly-valued audit blocks called sentinels. The verifier challenges the un-trusted server by describing the locations of a collection of sentinels and asking the untrusted server to return the associated sentinel values.

To support dynamic operations on data [4] presented a correct PDP mechanism based on symmetric keys. This mechanism can support update and remove the operations on data; however, insert operations are not available in this mechanism. Since it the achievement of symmetric keys to confirm the trustworthiness of information, it is not freely irrefutable and just gives a client a limited quantities of check solicitations.

In [6] designed to improved POR schemes. The primary plan is worked from BLS marks, and the second one depends on pseudorandom capacities. Wang et al. [3] can protect clients' private information from the TPA by utilizing arbitrary maskings. Likewise, to work the numerous inspecting undertakings from various clients effectively, they proceeded with their component to empower group examining by utilizing total marks [5].

The public mechanism proposed by [6] leveraged homomorphic tokens to assure the efficient of erasure codes-based data assigned on multiple servers. This

mechanism is adept not only to backing dynamic operations on data, but also to identify misbehaved servers. To minimize communication over in the phase of data repair, [7] also introduced a mechanism for verifying the correctness of data with the multi-server scenario, where these data are encoded through network coding instead of using erasure codes. More recently, in [8] composed an LT codes-based secure and reliable cloud storage mechanism. Examine the previous work [6, 7] this structure can avoid high decoding computation charge for data users and save computation resource for online data owners during data repair.

Wang et al. utilized Merkle Hash Tree and BLS signatures [9] to support fully dynamic operations in a public verifying mechanism. In [8] introduced dynamic provable data possession (DPDP) by using authenticated dictionaries, which are depending on rank information. Zhu et al. exploited the fragment system to reduce the storage of signatures in their public auditing mechanism. Likewise, they additionally utilized record hash tables to give dynamic operations to clients.

To maintain a strategic distance from unique assaults exist in remote information stockpiling framework with deduplication, [9] presented the documentation of evidences of-proprietorship (POWs), which enables a customer to demonstrate to a server that she really holds an information record, on the other hand only some hash estimations of the information document. In [10] additionally examined that POW and PDP can exist together under a similar system. As of late, in [11] proposed an unmindful outsourced stockpiling plan in light of Oblivious RAM procedures, which can conceal clients' get to designs on outsourced information from an unconfided in cloud. In [12] use rearranges record structure to ensure clients' get to designs on outsourced information.

We make sense of the plot assault in the leaving plan and give an effective open respectability evaluating plan with secure gathering client denial in light of vector duty and the verifier-nearby repudiation aggregate mark. We outline a solid plan in view of the plan definition. Our scheme supports the public checking and efficient user revocation and also few nice properties, such as confidently, correctness, accountability and traceability of secure group user revocation.

3.System model

The users are able to access and to share resources offered by cloud service providers at a lower marginal expenditure. It is routine for users to leverage cloud storage services to share data which remains in a group, as data sharing becomes standard feature in most cloud storage offerings, including Dropbox, iCloud and Google Drive. A system model composed of three major entities

1. The Cloud server
2. The Third party auditor [TPA]
3. Users

There are two category of users in a groups

1. The original user (master user)
2. The no. of group users

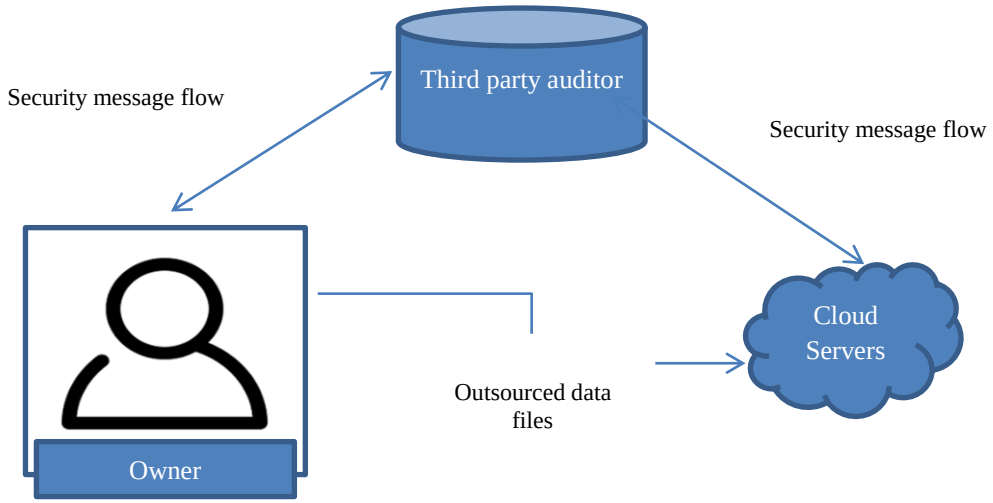

Figure 2 System model

The original user and the no. of group user are both associate of the group. The group associate can modify shared data created by the original user based on the controlled policy. Shared data and its verification information (i.e. signature) are both stored in the cloud server. The TPA refers to any party that check that integrity of data which is stored on the cloud.

Figure 2 shows the system model. Figure 3 shows the cloud proposed model. Figure 4 shows the flow diagram.

The conventional shape for checking information accuracy is to recover the full information from the cloud, and afterward confirm the information trustworthiness by checking the rightness of marks (e.g., RSA) or hash values (e.g., MD5) of the entire data. Certainly, this conventional approach able to successfully analysis the accurate of the cloud data.

4. Problem identification

In this work, focusing on the serious issues of identity revocation, we introduce public verification which checks data integrity not only by data owners, but also by any third party auditor. However dynamic schemes focus on data owner and data owner can modify the data. To protect the confidential data, it is essential and critical top reserve status of privacy from public verifiers during public auditing. In our protypical, privacy is accomplished by allowing the parties to upload their information in multi clouds and information is split into multiple parts so it gives more protection. The critical reasons due to which our above system is beneficial as:

1. Current working scenario involves Data analysis and verification.
2. Data Storage is path to mitigate the privacy concern.
3. Unauthorized users can leak or misuse the data; this problem still remains due to the based work.

The cloud specialist co-ops deal with an endeavor class framework that offers a versatile, secure and solid condition for clients, at a much lower negligible charge because of the sharing way of assets.

5. Proposed methodology

In proposed methodology, mainly focused on security enhancement using Identity-Based Encryption with added a secret Data key & Owner key to improve the user security, in demand to provide privacy in accessing the user data stored on cloud. In this proposed system, work and improvement done in two areas:

a. Security Enhancement:
b. Encryption Algorithm:

File Auditing

If an user edited an data then the auditor will monitor the user and report to the owner about the edited data . the group manager will monitored the changes in the file and if he found any discrepancy auditor has right to evocate from his particular group public auditor can audit the integrating of shared data without retrieving full data from a cloud even if some blocks in shared data have been resigned by a cloud.

Re-Assigning

On one hand, once our user is revoked from the group the block signed by the revoked user can be effectively resigned. The proxy is easy to convert a signature of Alice in to a signature of bob on the same block .Mean while the proxy is not able to learn any private keys of the two users which mean any cannot sign any block on favour of either Alice or bob.

File Upload

File owner allowed uploading data on the cloud either for their private or public use they act as a group manager for the file they upload in cloud. Both the original user and group user are easy to access download and modify shared data. Shared data is divided in to a no of blocks a user in the group can modify a blocks. in shared data can performed and insert, delete or update operation on the block.

Group Sharing

Data owner will save their data in a cloud and share the data among the group members. To upload the data have rights to modify and download their data in the cloud .

Access Control

The cloud server allowed only the certified group member to save the data in the cloud offer by cloud service provider.

User Revocation

The user revocation is secure because only existing users are easy to sign the blocks in shared data. Even with a resigning key a cloud which cannot generate a valid signature for arbitrary block on favor of an existing user.

6. Proposed block diagram

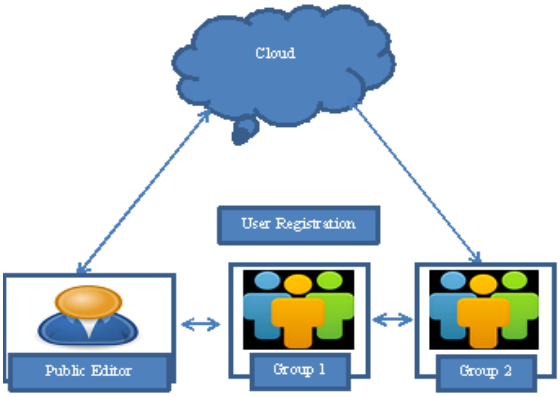

Figure 3 Cloud proposed model

Group user upload his data on cloud and shared it within group and another group , than public verifier is nothing but the group admin who can provide verification services to maintain integrity of data on cloud.

1. Current working scenario involves Data analysis and verification.
2. Data Storage is path to mitigate the privacy concern.
3. Unauthorized users can disclosed or misuse the data, this problem still remains due to the based work.

User has to registered in user registration, after that user login and can upload file and can check upload by checking in view data which required Data key.

7. Proposed flow diagram

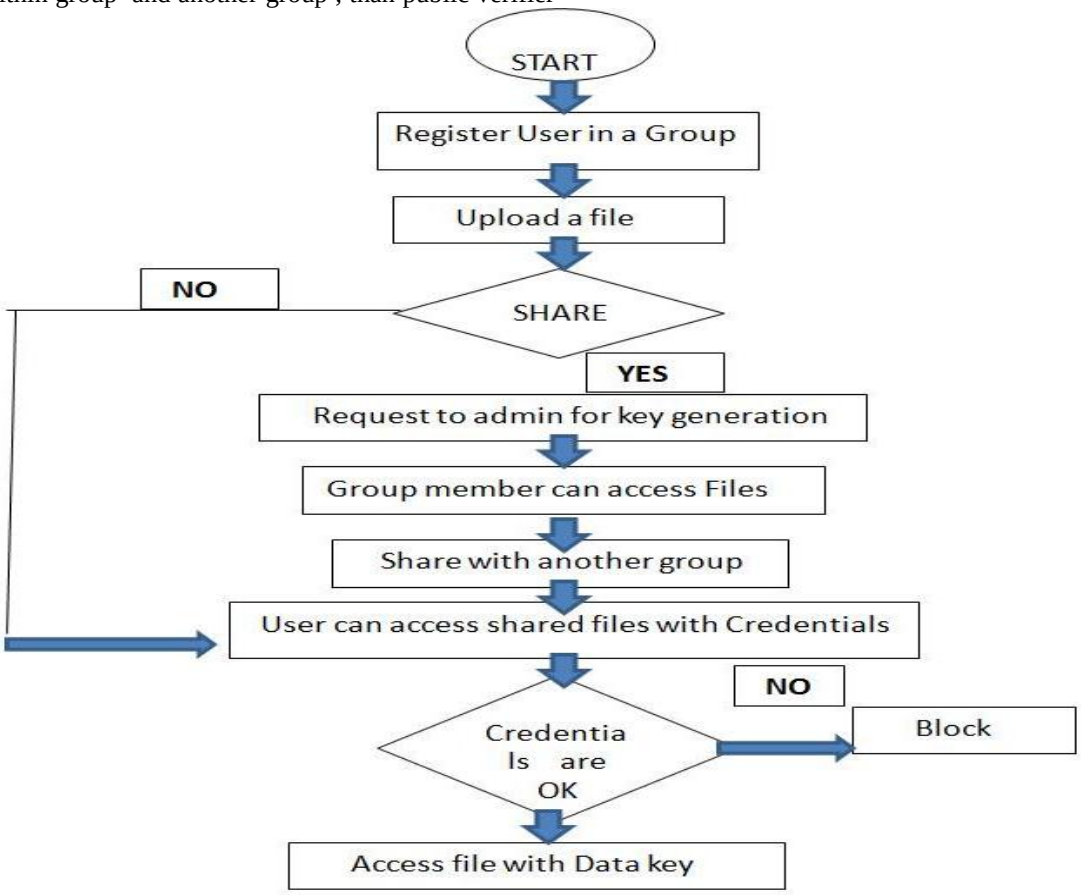

Figure 4 Flow diagram

8. Results

1.Install jdk 1.7 and above version
2.Install myself with ***admin*** password
3.Install net beans 8.0 with tomcat
4.Established connection through JDBC.
5.Open the source code find filename db.sql
6.Open in wordpad
7.Copy the file data and paste into mysql command prompt
8.In net beans then go for file->open project->then move to your project location->globe symbol appear->select it ->and click on open button.
9.Right tick on the project in net beans project explorer->properties->libraris->rmove the red colored libraries
10.Import all those packets which is required for our project
11.And click on button leftside->add externel jars->in each and every project having its own li folder open it.
12.Click on ok
13.Right click on the project run
14.Then execute the project...

Table 1Comparison table

Particulars	**Existing system**	**Proposed system**
Security of Data	Single Level Security	Multi-Level Security with Cloud Key and Owner Key
User Revocation	Revoke Manually (By Admin)	Automatic Revocation on Wrong Credentials
Data Confidentiality	User can see shared data only	Shared Data/File Accessible with Security Credentials only

Particulars	**Existing system**	**Proposed system**
Access Permission	On Request of Group User	On Request of Group User
Accessibility of Shared Data/File	Data Key will be Required	Owner Key as well as Cloud Key will be required
Auditor Role	Third Party Auditor for Data	Third Party Auditor for Data having Editing Rights for Documents
Admin Control	Block and Activate User	Activate User, Blocking will be done Automatically
User Control	Send request for files access and upload own files/data, Share it, View Group Files	Send request for files access and upload own files/data, Share it, View Group Files

The time analysis of the proposed system is carried out with different data items or blocks to calculate the time cost.

The comparison of time cost of query, verify time and update time is shown in the Figures 5, 6 and 7 respectively. From the time cost analysis it can be analyzed that the proposed (our scheme) has lower cost than the previous scheme [1]. Updated time costs are shown in Figures 8, 9 and 10. Table 1 shows the comparison. Table 2, 3 and 4 shows the query and verify time cost.

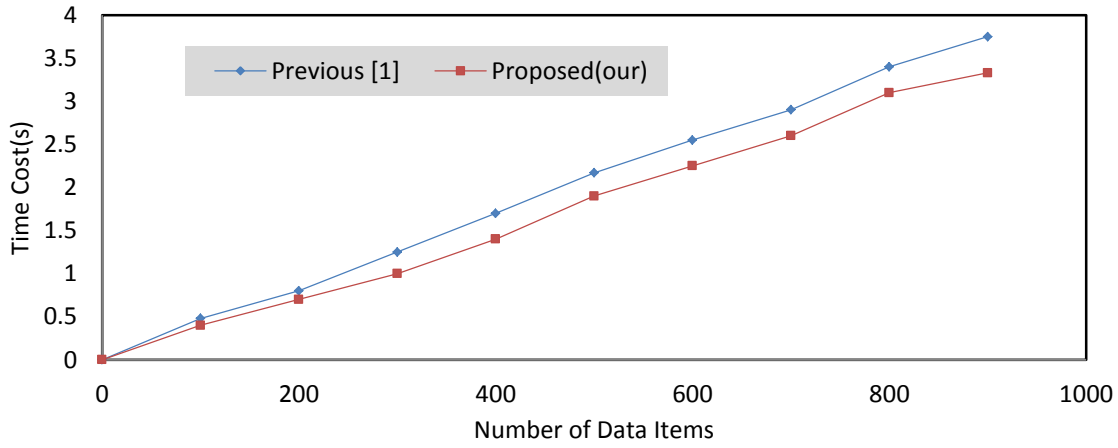

Figure 5 Query time cost

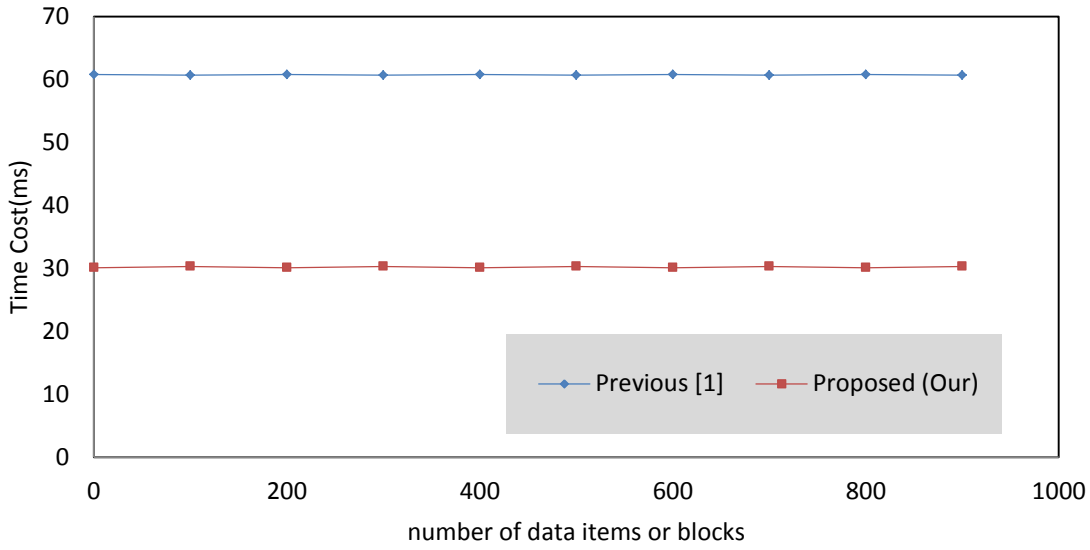

Figure 6 Verify time cost

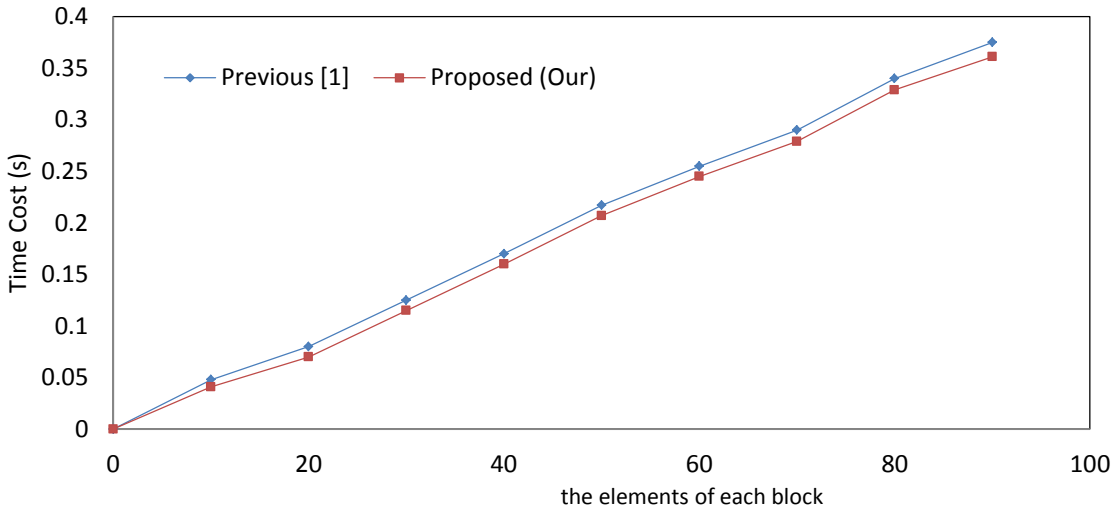

Figure 7 Update time cost

Table 2 Query time cost

No. of data items	Previous time	Proposed time
0	0	0
100	0.48	0.4
200	0.8	0.7
300	1.25	1
400	1.7	1.4
500	2.17	1.9
600	2.55	2.25
700	2.9	2.6
800	3.4	3.1
900	3.75	3.33

Table 3 Verify time cost

No. of data items	Previous time	Proposed time
0	60.8	30.1
100	60.7	30.3
200	60.8	30.1
300	60.7	30.3
400	60.8	30.1
500	60.7	30.3
600	60.8	30.1
700	60.7	30.3
800	60.8	30.1
900	60.7	30.3

Table 4 Update time cost

No. of data items	Previous time	Proposed time
0	0	0
10	0.048	0.041
20	0.08	0.07
30	0.125	0.115
40	0.17	0.16
50	0.217	0.207
60	0.255	0.245
70	0.29	0.279
80	0.34	0.329
90	0.375	0.361

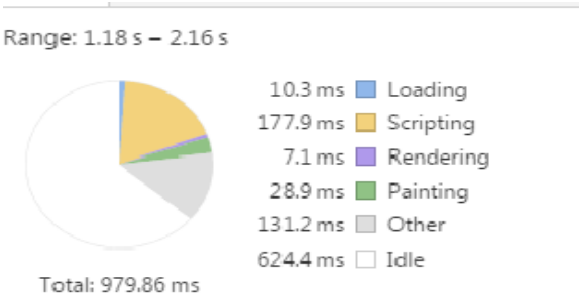

Figure 8 Query time cost

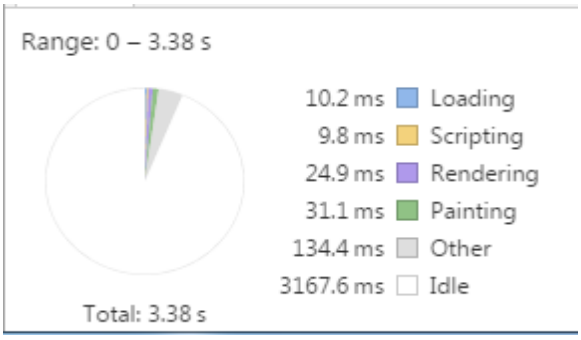

Figure 9 Verify time cost

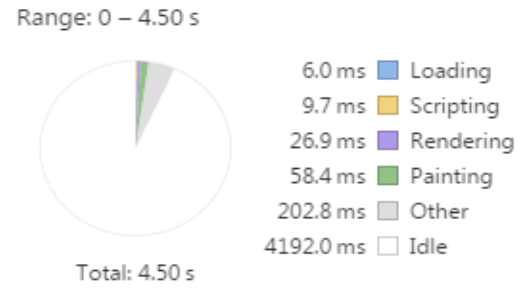

Figure 10 Update time cost

9. Conclusion and future work

In this research study the multiple layers has been analyzed through the system design. Security of user shared data has been increased the above results shows the system performance reached to the optimum value and the comparison table has been presented. We utilizing, the privacy preserving which shared the data in the cloud storage service that support the ring signature and Homomorphic authentication ring signature. It will easily audit the integrity of shared data. Our future work is how to audit shared data with dynamic members although users sharing the data it will be safe. Utilizing privacy preserving who shared the data in the cloud storage service with the aid of rising signature it will easily audit the integrity of shared data. In future shared data can audit with dynamic members while the users sharing the data. It also provides the privacy to users for saving their confidential file on a cloud and using ownercloud key and owner key after that user can access the file. In this disquistion, stages of security are increased. In observance of all the parameters, in future we can add other security to improve this system by adding various new techniques to enhance more stages of security. Some another algorithms can further be used to provide more perfection and security to the system.

References

[1] Jiang T, Chen X, Ma J. Public integrity auditing for shared dynamic cloud data with group user revocation. IEEE Transactions on Computers. 2016; 65(8):2363-73.

[2] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, Song D. Provable data possession at untrusted stores. In proceedings of the 14th ACM conference on computer and communications security 2007 (pp. 598-609). ACM.

[3] Wang C, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for data storage security in cloud computing. In infocom, 2010 proceedings IEEE 2010 (pp. 1-9). IEEE.

[4] Rivest RL, Shamir A, Tauman Y. How to leak a secret. In international conference on the theory and application of cryptology and information security 2001 (pp. 552-65). Springer Berlin Heidelberg.

[5] Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In international conference on the theory and applications of cryptographic techniques 2003 (pp. 416-32). Springer Berlin Heidelberg.

[6] Shacham H, Waters B. Compact proofs of retrievability. In international conference on the theory and application of cryptology and information security 2008 (pp. 90-107). Springer Berlin Heidelberg.

[7] Zhu Y, Wang H, Hu Z, Ahn GJ, Hu H, Yau SS. Dynamic audit services for integrity verification of outsourced storages in clouds. In proceedings of the 2011 ACM symposium on applied computing 2011 (pp. 1550-7). ACM.

[8] Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable, and fine-grained data access control in cloud computing. In infocom, 2010 proceedings IEEE 2010 (pp. 1-9). IEEE.

[9] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. In international conference on the theory and application of cryptology and information security 2001 (pp. 514-32). Springer Berlin Heidelberg.

[10] Boneh D, Freeman DM. Homomorphic signatures for polynomial functions. In annual international conference on the theory and applications of cryptographic techniques 2011 (pp. 149-168). Springer Berlin Heidelberg.

[11] Ferrara AL, Green M, Hohenberger S, Pedersen MØ. Practical short signature batch verification. In cryptographers' track at the rsa conference 2009 (pp. 309-24). Springer Berlin Heidelberg.

[12] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. In proceedings of the 13th ACM conference on Computer and communications security 2006 (pp. 89-98). ACM.