International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 7, July 2020||

Secure Group Sharing and Fine Grained Conditional Distribution with Multiple Owner in Cloud Computing

Jondhale Dhanashree Rajaram, Prof.Rokade.S.M

Department of Computer Engineering, Pravara Rural Engineering College, Loni, Maharastra, India

ABSTRACT: In the proposed System users can achieve an effective and economical approach for data sharing among group members in the cloud with characters of low maintenance and little management cost. Proposed system will provide security for the sharing data files since they are outsourced .In existing system the secure key distribution is based on secure point .Dynamic group sharing is a scheme which used in existing system and private keys are shared only within group members. Group members can securely obtain their private key from group Manager.The System can accomplish two factor fine grained access control and also system protect from collusion attack which means user upload the same name of file same group or different group then collusion attack by Name.When User or group manager revoke from dynamic group then group of all member key will compulsory be updated due to point of security also to be a classified member of the group user has to upload at least one file to detect fake users and to maintain data integrity.

KEYWORDS: Access Control, Cloud Computing, Group Sharing,Key Distribution, Privacy-Preserving

I.INTRODUCTION

Disseminated registering is an Internet-based figuring form that gives PC shared PC planning resources and data and diverse devices on ask. It is a figuring style where capably versatile and consistently virtualized resources are given as an Internet advantage. A champion among the most basic organizations offered by cloud providers is data storing. Allow us to consider an utilitarian data application. An association allows its delegates in a comparative social affair or division to archive and offer records in the cloud. In any case, it similarly addresses a basic risk for the security of set away records. An association empowers its staff to be in a comparative social event or division to record and offer archives in the cloud. Regardless, it moreover addresses a tremendous peril for the mystery of set away reports. In particular, cloud-supervised cloud servers are not trusted by customers, and data records set away in the cloud can be unstable and fragile, for instance, techniques for progress. To safeguard data security, a major course of action is to scramble data records and exchange encoded data to the cloud. Character assurance is a champion among the hugest hindrances to the sweeping use of conveyed registering. Without the affirmation of identity assurance, customers may not join disseminated figuring structures in light of the fact that their certified characters could without a doubt be revealed to cloud providers and Attackers. On the other hand, inadequate security of identity may result in insurance misuse.

For example, the wrong staff can trap others into the association by sharing imposter records without being taken after. Thu-sly, trace ability, which empowers the social occasion director to reveal the confide identity of a customer, is in like manner extremely appealing. It is recommended that all people from a social event can value full dispersed stockpiling and sharing organizations, described as multi-proprietor mode. Stood out from the extraordinary proprietor mode, where simply the social affair director can store and modify data in the cloud, proprietor various mode is more versatile in rational applications. Specifically, every customer in the social occasion can read the data, and in addition change their bit of the data over the entire data archive shared by the association. Finally, bundles are regularly interesting eventually, for example, another laborer affiliation and the present delegate refusal in an association. Changing branches makes it to a great degree difficult to exchange data. From one viewpoint, the secretive system challenges new customers to know the substance of the set away data reports before they take an enthusiasm, as it is stunning for new customers to contact obscure data proprietors and get their unscrambling keys. On the other hand, you also require a practical part repudiation segment without invigorating the riddle keys of remarkable customers to restrain the multifaceted idea of key organization. A couple of security designs have been proposed

for data sharing and lie servers. In these strategies, data proprietors store the mixed data records in a trusted in anal and scatter the relating disentangling.

B. GOALS AND OBJECTIVES

1) The main goals of the proposed scheme includes access control, data confidentiality, anonymity and trace ability and efficiency.
2) To achieve Access Control within the group private keys are generated for every user to provide access to files.
3) To achieve data confidentiality after revocation of any member the private keys of existing members of that group will be updated.
4) To maintain the private keys of every user and provide them access to their resources without any Certificate Authorities.

II. LITERATURE REVIEW

1) The cloud supplier a standout amongst other administrations is information stockpiling the security and protection issue have real worry for association for using such administration. Cloud information stockpiling has given critical advantages by enabling clients to store monstrous measure of information on request in a financially savvy way. To secure the protection of information put away in the cloud, cryptographic part based access control (RBAC) plans have been created to guarantee that information must be gotten to by the individuals who are permitted by get to arrangements. Be that as it may, these cryptographic methodologies don't address the issues of trust. In this paper, we propose trust models to reason about and enhance the security for put away information in distributed storage frameworks that utilization cryptographic RBAC plans. The trust models give a way to deal with the proprietors and parts to decide the dependability of individual parts and clients separately in the RBAC framework. The proposed trust models think about part legacy and order in the assessment of dependability of parts. We introduce a plan of a trust-based distributed storage framework which indicates how the trust models can be coordinated into a framework that utilizations cryptographic RBAC plans. We have likewise thought to be functional application situations and represented how the trust assessments can be utilized to decrease the dangers and upgrade the nature of basic leadership by information proprietors and parts of distributed storage benefit[1].

2) Distributed computing, the long-held dream of registering as an utility, can possibly change a substantial piece of the IT business, making programming significantly more alluring as an administration and molding the manner in which IT equipment is outlined and obtained. Designers with inventive thoughts for new Internet benefits never again require the substantial capital costs in equipment to convey their administration or the human cost to work it. They require not be worried about finished provisioning for an administration whose prominence does not meet their expectations, in this manner squandering exorbitant assets, or under provisioning for one that turns out to be uncontrollably mainstream, along these lines missing potential clients and income. Distributed computing alludes to the utilization of Internet ("cloud") based PC innovation for an assortment of administrations. It is a processing model in which virtualized assets are given as an administration over the Internet. The idea consolidates foundation as an administration (IaaS), stage as an administration (PaaS) and programming as an administration (SaaS) that have the normal topic for fulfilling the figuring needs of the clients. Distributed computing administrations more often than not give normal business applications online that are gotten to from an internet browser. This paper gives careful consideration to the Grid worldview, as usually mistook for Cloud innovations. We likewise de-copyist the connections and qualifications between the Grid and Cloud approaches[2].

3) We consider the issue of building a protected distributed storage benefit over an open cloud framework where the specialist organization isn't totally trusted by the client. We depict, at an abnormal state, a few structures that join later and non-standard cryptographic natives keeping in mind the end goal to accomplish our objective. We review the advantages such an engineering would give to the two clients and specialist co-ops and give a diagram of ongoing advances in cryptography roused particularly by distributed storage[3].

4) A safe document framework intended to be layered over unreliable system and P2P record frameworks, for example, Folder case.. Key administration and repudiation is straightforward with negligible out-of-band correspondence. Document

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 7, July 2020||

framework freshness ensures are upheld by SiRiUS utilizing hash tree developments. SiRiUS contains a novel technique for performing record sporadic access in a cryptographic report structure without the use of a square server. Extensions to SiRiUS fuse huge scale gather sharing using the NNL key renouncement advancement. Our execution of SiRiUS performs well as for the concealed record structure despite using cryptographic exercises[4].

5) Enhanced intermediary re-encryption plans with applications to anchor dispersed capacity. We foresee that fast and secure re-encryption will end up being dynamically popular as a method for regulating mixed record systems. Though capably measurable, the unlimited apportionment of BBS re-encryption has been forestalled by great security risks. Following continuous work of Dodis and Ivan, we show new re-encryption plots that comprehend a more grounded idea of security, and we demonstrate the estimation of mediator re-encryption as a method for adding access control to a protected record system. Execution estimations of our test record structure show that
delegate re-encryption can work effectively done[5].

6) Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption, This advances new effective developments for open key communicate encryption that at the same time appreciate the accompanying properties: beneficiaries are stateless encryption is intrigue secure for discretionarily expansive arrangements of clients and security is tight in the standard model; new clients can join powerfully i.e. without adjustment of client unscrambling keys nor figure content size and next to zero modification of the encryption key. We additionally demonstrate to for all time deny any subgroup of clients. In particular, our developments accomplish the ideal bound of O(1)-measure either for figure writings or unscrambling keys, where the shrouded consistent identifies with two or three components of a blending well disposed gathering. Our communicate KEM trapdoor method, which has free intrigue, additionally gives a dynamic communicate encryption framework enhancing all past productivity measures (for both execution time and sizes) in the private-key setting[6].

7) Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing, It is a greatest stage that gives data storing in especially lesser cost and record-breaking it should be open over the web. The security must be basic in the circulated processing. The encryption method is generally grasped by the conveyed processing that suggests the encoded data should be secured on the limit of cloud to anchor the data. Encryption is no sufficient as affiliation gain need to maintain fine-grained get the opportunity to control on data. Such control relies upon the trademark that structure is known as the property based system. For the data security it is basic to encode the data and exchange the mixed data on the cloud. In cloud it is hard to design powerful and secure data sharing arrangement in multi proprietor structure on account of the going with testing issues. Identity, repudiation and new part bolster i.e. the movements of investment make securely data sharing to an extraordinary degree troublesome. On the other hand a gainful part repudiation without reviving the riddle key of remarkable customer to restrain the multifaceted idea of key organization. Stamped receipt is caused after each part disavowal in total that breaking points distinctive copy of encoded record it can restrict estimation cost[7].

8) Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud , Displayed cryptographic limit structure that engage secure data sharing. In this technique isolating report into the record assembling and scramble each archive store up with a record square key. In this arrangement at the period of customer denial the record square key ought to be revived and circled to the customer henceforth the structure had a generous key scattering overhead. Plutus is a cryptographic accumulating structure that enables secure record sharing without setting much trust on the archive servers. In particular, it makes novel use of cryptographic locals to guarantee and offer records. Plutus incorporates uncommonly versatile key organization while empowering singular customers to hold manage control over who picks up permission to their archives. We illuminate the segments in Plutus to reduce the amount of cryptographic keys exchanged between customers by using filegroups, perceive record read and create get the chance to, handle customer repudiation capably, and allow an untrusted server to endorse archive forms. We have created a model of Plutus on OpenAFS. Estimations of this model show that Plutus achieves strong security with overhead identical to structures that scramble all framework development[8].

9) Circuit Cipher text – procedure Attribute based Hybrid encryption with verifiable Delegation in conveyed processing. In the cloud, for achieving access control and keeping data mystery, the data proprietors could get credit based encryption to scramble the set away data. Customers with limited handling power are in any case more slanted to assign the cloak of the deciphering undertaking to the cloud servers to reduce the figuring cost. In like manner, characteristic based encryption with assignment rises. Everything considered, there are stipulations and request remaining in the past critical works. For instance, in the midst of the arrangement, the cloud servers could change or supplant the assigned figure message and respond a formed handling result with dangerous objective. They may in like manner cheat the qualified customers by responding them that they are ineligible with the true objective of cost saving. Besides, in the midst of the encryption, the passageway techniques may not be adequately versatile as well. Since course of action for general circuits engages to achieve the most grounded sort of access control, an advancement for recognizing circuit figure content approach property based mutt encryption with irrefutable arrangement has been considered in our work. In such a structure, joined with certain figuring and scramble then-mac framework, the data protection, the fine-grained get the opportunity to control and the rightness of the doled out preparing results are all around guaranteed meanwhile. In addition, our arrangement achieves security against picked plain text attacks under the k-multi coordinate Decisional Diffie-Hellman supposition. Additionally, a wide reenactment fight certifies the feasibility and efficiency of the proposed plan[9].

10) Fine Grained Two Factor Access Control for web based cloud computing Services. In our proposed 2FA access control structure, a quality based access control instrument is completed with the need of both a customer puzzle key and a lightweight security device. As a customer can't get to the system if they don't hold both, the Mechanism can enhance the security of the structure, especially in those circumstances where various customers share a comparative PC for electronic cloud organizations. Besides, quality based control in the structure also enables the cloud server to restrict the passageway to those customers with a comparable course of action of properties while sparing customer security, i.e., the cloud server just understands that the customer fulfills the required predicate yet has no idea on the right identity of the customer. Finally, we in like manner finish an amusement to display the practicability of our proposed 2FA system[10].

11) Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption, This advances new effective developments for open key communicate encryption that at the same time appreciate the accompanying properties: beneficiaries are stateless encryption is intrigue secure for discretionarily expansive arrangements of clients and security is tight in the standard model; new clients can join powerfully i.e. without adjustment of client unscrambling keys nor figure content size and next to zero modification of the encryption key. We additionally demonstrate to for all time deny any subgroup of clients. In particular, our developments accomplish the ideal bound of O(1)-measure either for figure writings or unscrambling keys, where the shrouded consistent identifies with two or three components of a blending well disposed gathering. Our communicate KEM trapdoor method, which has free intrigue, additionally gives a dynamic communicate encryption framework enhancing all past productivity measures (for both execution time and sizes) in the private-key setting[11].

12) Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing, It is a greatest stage that gives data storing in especially lesser cost and record-breaking it should be open over the web. The security must be basic in the circulated processing. The encryption method is generally grasped by the conveyed processing that suggests the encoded data should be secured on the limit of cloud to anchor the data. Encryption is no sufficient as affiliation gain need to maintain fine-grained get the opportunity to control on data. Such control relies upon the trademark that structure is known as the property based system. For the data security it is basic to encode the data and exchange the mixed data on the cloud. In cloud it is hard to design powerful and secure data sharing arrangement in multi proprietor structure on account of the going with testing issues. Identity, repudiation and new part bolster i.e. the movements of investment make securely data sharing to an extraordinary degree troublesome. On the other hand a gainful part repudiation without reviving the

riddle key of remarkable customer to restrain the multifaceted idea of key organization. Stamped receipt is caused after each part disavowal in total that breaking points distinctive copy of encoded record it can restrict estimation cost[12].

13) Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud , Displayed cryptographic limit structure that engage secure data sharing. In this technique isolating report into the record assembling and scramble each archive store up with a record square key. In this arrangement at the period of customer denial the record square key ought to be revived and circled to the customer henceforth the structure had a generous key scattering overhead. Plutus is a cryptographic accumulating structure that enables secure record sharing without setting much trust on the archive servers. In particular, it makes novel use of cryptographic locals to guarantee and offer records. Plutus incorporates uncommonly versatile key organization while empowering singular customers to hold manage control over who picks up permission to their archives. We illuminate the segments in Plutus to reduce the amount of cryptographic keys exchanged between customers by using filegroups, perceive record read and create get the chance to, handle customer repudiation capably, and allow an untrusted server to endorse archive forms. We have created a model of Plutus on OpenAFS. Estimations of this model show that Plutus achieves strong security with overhead identical to structures that scramble all framework development[14].

14) Circuit Cipher text – procedure Attribute based Hybrid encryption with verifiable Delegation in conveyed processing. In the cloud, for achieving access control and keeping data mystery, the data proprietors could get credit based encryption to scramble the set away data. Customers with limited handling power are in any case more slanted to assign the cloak of the deciphering undertaking to the cloud servers to reduce the figuring cost. In like manner, characteristic based encryption with assignment rises. Everything considered, there are stipulations and request remaining in the past critical works. For instance, in the midst of the arrangement, the cloud servers could change or supplant the assigned figure message and respond a formed handling result with dangerous objective. They may in like manner cheat the qualified customers by responding them that they are ineligible with the true objective of cost saving. Besides, in the midst of the encryption, the passageway techniques may not be adequately versatile
as well. Since course of action for general circuits engages to achieve the most grounded sort of access control, an advancement for recognizing circuit figure content approach property based mutt encryption with irrefutable arrangement has been considered in our work. In such a structure, joined with certain figuring and scramble then-mac framework, the data protection, the fine-grained get the opportunity to control and the rightness of the doled out preparing results are all around guaranteed meanwhile. In addition, our arrangement achieves security against picked plain text attacks under the k-multi coordinate Decisional Diffie-Hellman supposition. Additionally, a wide reenactment fight certifies the feasibility and efficiency of the proposed plan[15].

15) Fine Grained Two Factor Access Control for web based cloud computing Services. In our proposed 2FA access control structure, a quality based access control instrument is completed with the need of both a customer puzzle key and a lightweight security device. As a customer can't get to the system if they don't hold both, the Mechanism can enhance the security of the structure, especially in those circumstances where various customers share a comparative PC for electronic cloud organizations. Besides, quality based control in the structure also enables the cloud server to restrict the passageway to those customers with a comparable course of action of properties while sparing customer security, i.e., the cloud server just understands that the customer fulfills the required predicate yet has no idea on the right identity of the customer. Finally, we in like manner finish an amusement to display the practicability of our proposed 2FA system[16].

III. PROPOSED METHODOLOGY

In the Proposed System a secure Group sharing scheme which can achieve through a secure key distribution and data sharing for dynamic group along with secure. New re encryption is used for assigning the permission data encryption. The Users can securely obtain there Private Key from group Manger with. The System can achieve the two level securities. Hybrid cloud is used for efficient use of cloud. Our System used for data sharing can be protected from collusion attack. The Revoked user not gets the original data access once when they revoked from particular even if they tried with untruth cloud. System

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 7, July 2020||

supports the dynamic group efficiently when user joins the group or revoked from group their private key are compulsory update and recomputed.

After that Uploading into Register groups than user are revoke from group then private key of all member' s key are updated by Algorithms.

Advantages of Proposed System:

1) If user can access the data from other group then group Member are called as the fake user and that user Group Member are revoke from Application.
2) If user revokes from register group then compulsory updated their group's member private key.
3) We improve data security using ECC(Elliptic curve cryptography) and Block Generation algorithms.

A. Architecture

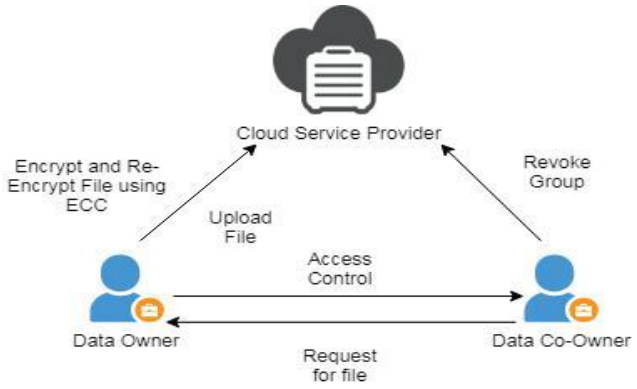


Fig. 1. Proposed System Architecture

Dynamic Groups:

The Main Concepts of Dynamic Group users select the Partic-ular group when user Register with Group. Groups are created by the Group Manger.

User Revoked or User Join:

When new user joins or revoked from particular group then the Private Key of particular user and other user of same group their private key compulsory update and recomputed.

Group Manger:

Group Manger is created the Groups. And Manger decided space of group and Dynamical efficiently used space.

B. Algorithms

1. Elliptic curve cryptography

Encryption has become a part and parcel of our lives and we have accepted the fact that data is going to encrypted and decrypted at various stages. However, there is not a single encryption algorithm followed everywhere. There are a number of algorithms existing, and I feel there is a need to understand how they work. So this text explains a number of popular encryption algorithms and makes you look at them as mathematical formulas

Input:

1. 128 bit /192 bit/256 bit input(0,1)
2. secret key(128 bit)+plain text(128 bit). Process:
3. 10/12/14-rounds for-128 bit /192 bit/256 bit input
4. Xor state block (i/p)
5. Final round:10,12,14
6. Each round consists:sub byte, shift byte, mix columns, add round key.

Output:

cipher text(128 bit)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 7, July 2020||

2. Block Generating (v, k+1, 1) :- generating a new block

1) for i=0;i¡=k;i++ do
2) for j=0;j¡=k;j++ do
3) if j==0 then
4) Bi,j=0; else
5) bi,j=ik+j;
6) end if
7) end for
8) end for
9) for i=k+1 ;i¡=k +k ;i++ do
10) for j=0;j¡k ;j++
11) j==0 then
12) Bi,j=[(i-1)/k +1]
13) Else
14) Bi.k=jk+1 +Mod k+1(i-j+(j-1)[i-1]/k+1)
15) End if
16) End for
17) End for

C. Mathematical Model
ID_i is the Identity of user i ID_{datai} is the Identity of Data i
pk the Public key of user that Needs to be Negociated with group manager
sk corresponding private key to pk
KEY = (x_i; A_i; B_i) the Private key which is distributed to user from group manager and user data Sharing.
EN C_k Symmetric encryption algorithms used the encryption key k
AEN C_k Asymmetric encryption algorithms used for encryption key k
UL user group list
DL data list
The group manager selects a random number xi Z_Q and computes the following equations

$$^{8}B_i = x^{y+i} \quad G \quad G_1 \qquad (1)$$

$$A_i = \frac{1}{y+x_i} \quad P \quad 2\ G_1$$

$$> \quad i \quad 2$$

$$<$$

$$^{>}V_i = \frac{x}{f(B_i)}$$

:
(x_i; A_i; B_i) constructs the message KEY:

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 7, July 2020||

2. File Upload:

$$\begin{cases} C_2 = kP \quad 2G_1 \\ C_1 = k \quad Y \quad G_1 \\ K = Z^K \quad 2 \quad G_2 \\ C = ENC_K(M) \end{cases} \qquad (2)$$

$(x_i; A_i; B_i)$ constructs the message KEY:

3. File Downloading:

This operation is performed by the group member and the cloud, the group member encrypts IDdata with his key Ai and sends ID_group; ID_i; Enc_Ai(IDdata)as a request to the cloud. On receiving the message, the cloud decrypts it and compares the encryption key Ai with keys in the group user list, if the encryption key Ai is in the list, the cloud then sends the corresponding data file

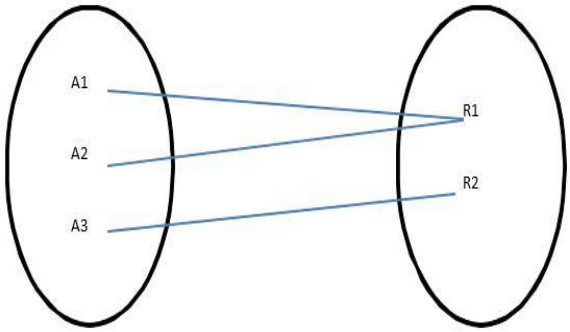
$$DF = (ID_group; ID_data; CE; EK; t_data); \quad DF \qquad (3)$$

4. Access Control:

The access control is based on the security of the group user list, which is signed by the group manager with his signature sig(UL) = yf1(UL) and this operation is generally performed by the cloud. The cloud verifies the identity of the group manager by checking the equation

$$e(W; f_i(U\,L)) = \begin{cases} e(P; f_i(UL)) \\ e(P; f(U\,L)) \end{cases} \qquad (4)$$

$$e(P; f_i(UL)) = e(P; sig(U\,L))$$



| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 7, July 2020||

IV. RESULT AND DISCUSSION

First of all, the group member chooses a unique data file identity ID data and a random number k $2Z_q$; then computes these parameters as the following equation:

We expect the comparison of some security parameters ODBE, Mona and our scheme. It is obviously observed that the computation cost for members in our scheme is irrelevant to the number of revoked users.

TABLE I
SECURITY PERFORMANCES COMPASSION

	Secure Key Distribution	Access Control	Secure user revocation	Anti Collusion attack
Mona	No	Yes	No	No
RBAC Scheme	No	Yes	No	No
ODBC Scheme	No	Yes	Yes	Yes
Our Scheme	Yes	Yes	Yes	Yes

TABLE II
SECURITY PERFORMANCES COMPASSION

Parameter	Exiting System	Proposed System
Cost	High	Low
Security access based	Low	High
ODBC Scheme	Yes	No
RBAC	No	Yes
Data Security	No	Yes
Access Control	Yes	Yes
User Revocation	No	Yes
Data Confidentially	No	Yes
Anti-Collision attack	No	Yes

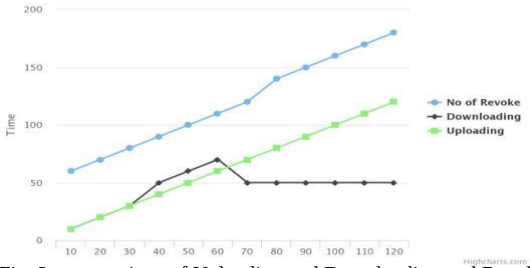


Fig. 2. comparison of Uploading and Downloading and Revoke

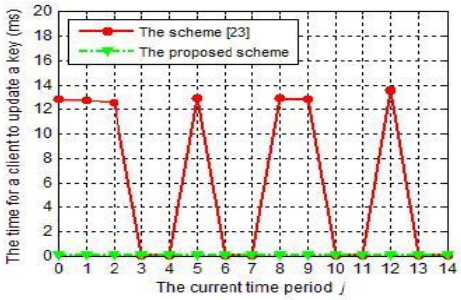


Fig. 3. Uploading Time for Updating Key

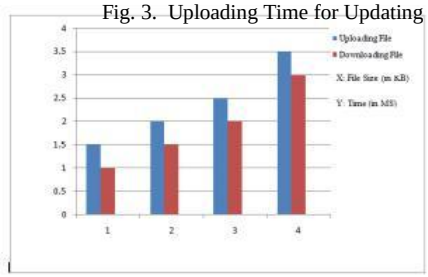


Fig. 4. Comparison of Uploading and Downloading of File Size

V. CONCLUSION

The system is design for secure data sharing scheme, for dynamic groups for security and privacy. In this system, present a secure group for data exchange Multi-owner cloud computing scheme. In our schema, the data owner could encrypt his private data and share them with a group of data access devices simultaneously time conveniently based on the proposed technique. The data owner can specify specific access encrypted text therefore, the encrypted text can be encrypted only by data diffuser whose attributes satisfy the access policy in the encrypted text.

Future Research: multi keyword search scheme over encrypted data.

REFERENCES

[1] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," IEEE Access, vol. 6, pp. 30049–30059, 2018.

[2] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.

[3] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 2017.

[4] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dis-semination with attribute and time conditions in Public Clouds," IEEE Transactions on Services Computing, 2018.

[5] L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," IEEE Access, vol. 5, pp. 13336 – 13345, 2017.

[6] S.Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.

[7] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010

[8] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[9] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.

[11] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size Ciphertexts or decryp-tion keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59.

[12] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun.Security, 2010, pp. 282–29.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 7, July 2020||