Protection for Multi Owner Data Sharing Scheme

K.B. Aruna, A. LallithaShri, Aravindh, Jayakumar and Jayasurya

Abstract--- *Cloud computing turns to be a service orientated computing technology to deliver storage and computing resources at reasonable worth over net. Since Clouds are getting matured, many enterprises square measure outsourcing their workloads by utilizing the cloud resources for the structure knowledge storage, deposit and operational usage. as a result of delivery of resources with service over Clouds, that can be accessed by multiple users United Nations agency may be house owners or finish users of the information As, there exists multiple house owners of the information, and therefore the knowledge can be changed or updated at the same time, this might cause several challenges in terms of knowledge organization, access and sharing, that differs from the traditional method of access/modifying the information. Hence, it's essential to supply many mechanisms in Cloud computing so permitting sharing of the information or resources among multiple users effectively could be a major challenge. during this paper, we have a tendency to discuss many mechanisms to deal with secured knowledge sharing problems and discuss the multiple house owners and teams issues in Clouds.*

Keywords--- *Access control,Cloud Computing, Encryption, Servers.*

I. INTRODUCTION

CLOUD computing is taken into account as an alternate to ancient information technology [1] thanks to its essential characteristics such as sharing of resources, and lowest operational and maintenance problems. knowledge storage is one among the service offered by cloud service suppliers, that has gained prominence in current world as a result of a client will store his knowledge at cheaper cost within the cloud. The good thing about knowledge storage is, it permits knowledge sharing and accessing among the cluster of individuals in a very additional secured and consistent approach. within the Recent survey by Information week[2] the majority organizations shared seventy four of their knowledge with customers or users and sharing sixty fourth with suppliers. think about Associate in Nursing example for knowledge sharing in a very social networking services like face book, wherever users will upload their photos, videos and alternative information's will share their knowledge with alternative users, the opposite example is cluster connected projects and students. knowledge sharing may be a helpful methodology in cloud environments, as an example think about a university scenario ,a faculty in a very department or cluster area unit allowed to store and share the files from the Cloud storage services.

II. RELATED WORK

Here, we tend to describe the importance of knowledge sharing and its requirements and edges.

A. Importance of Knowledge

For easy management of security ,groups square measure accustomed gathers users of comparable interest or of various roles. A group is outlined as assortment or collection of knowledge Owners appointed with a collection of permissions. Groups are principally targeted on users identities. knowledge sharing within thegroup has achieved bigger importance in multipledomains like business, governments and organizations inthe real world.

B. Necessities of Knowledge Sharing During a Cluster

- A knowledge owner ought to describe the list or cluster of users World Health Organization will access his knowledge
- A user during a cluster should have the correct to access the data at anytime from anyplace, while not knowledge owner permission.
- solely the members of the cluster and therefore the knowledge owner should have access to the information keep in cloud.
- No different th6an a knowledge owner has the permission to add a replacement member or user to a gaggle.
- a knowledge owner has the access to Revoke a user from a group.

C. Edges of Knowledge Sharing

- Higher profit
- Ease access
- To voice opinions

The two major obstacles in cloud computing are:

- Privacy : Privacy means that it's the power of storing the data or data and dominant it from others preventing from attack.
- Security : Security means that providing confidentiality, integrity and convenience for the information. In [3][4][5] planned knowledge sharing techniques for AN un trustworthy servers. during this ways, assumptive knowledge house owners or users store their knowledge in AN encrypted type on world organization trustworthy cloud servers and decipherment keys ar distributed in some secure form to the users, such permitting solely licensed users to access the shared knowledge in cloud. however a brand new member registration and revocation

K.B. Aruna.
A. LallithaShri.
Aravindh, S.A.Engineering College,Chennai.
Jayakumar, S.A.Engineering College,Chennai.
Jayasurya, S.A.Engineering College,Chennai.
DOI: 10.9756/BIJAIP.10485

mechanisms have higher complexities with the rise within the range of knowledge house owners and revoked users in cloud. lutecium et al[6] resolves the higher than problem by victimisation Cipher text ABE(CP-ABE)[7] how ever failed to addressed the opposite drawback of revocation of users . Yu et al.[8] planned a ascendable and fine -grained knowledge access management technique in cloud victimisation key policy Attribute primarily based encryption(KP-ABE).but this methodology is a lot of versatile to single knowledge owner.

It is not versatile and simple to style AN economical knowledge sharing method for multiple house owners in multiple teams for multiple users in a very secure manner.

In this paper we tend to study existing literature survey on secure and efficient knowledge sharing ways.

D. Problems with Data Sharing

- Confidentiality : The data owner stores his data or files in the cloud. If the servers in Cloud taken care by Cloud service providers, which are not completely trusted, allowing access to unauthorized users.
- Scalable and Efficient: A cloud have large numbers of users ,where any user in a group can dynamically add or leave from a group, it is critical to maintain the system efficient and scalability.
- User Revocation: When a user is revoked from agroup at any time ,it is essential to remove access todata ,without effecting other user in a group.
- Collusion between entities: When we analyzed data sharing methods in cloud, even though when entities collude ,none of the user should be able to access the data without permission of data owners

Confidentiality for the stored data is at risk, as the data in clouds is vulnerable to many attacks like privacy and security [9][10] because of un trusted servers at cloud providers. But nowadays sharing of data among groups as become an important and necessary approach. A basic approach to provide privacy for the users data is, a user or data owner in a group can encrypt and store their data in the cloud such that the cloud service provider or a non-member in a group cannot decrypt the data. Hence users data is an information theoretically secured from unauthorized users like cloud service providers and other d ,despite the fact that the weight is exchanged to the Cloud.E. Received Approaches :The few systems are examined in Table 1.

Property Based Encryption :- Attribute-Based Encryption (ABE) is an exceptional technique used to give fine-grained get the opportunity to control to data secure in the Cloud. Mainly an Access Control List (ACLs) is kept up ,which contains access to data in Cloud in any case, this was not versatile and in a manner of speaking given coarse-grained access to data [10]. Trademark Based encryption at first proposed by Goyal et al. [7] gives a more flexible what's more, fine-grained get the opportunity to control to data in connection to ACLs. Quality Based Encryption is a get the chance to control part where a customer or a touch of data has attributes related with it. A get the chance to control approach is portrayed and if the qualities satisfy the get the opportunity to control approach the customer should have the ability to get to the bit of data. There are two sorts of ABE [6], which are depicted takes after. : Key-Policy ABE (KP-ABE): In this approach, a get the chance to control game plan is secured with the customer's private key and the encoded data and also it stores different qualities related with the data. A customer can translate the data if and just if the qualities of the data satisfying the get the opportunity to control course of action in the customer's key. The get the chance to control course of action is addressed as a get the chance to tree structure with inside centers addressing limit portals with AND or possibly entryways and leaf centers addressing attributes.

Cipher content Policy ABE (CP-ABE): The CP-ABE is backwards of KP-ABE. The get the opportunity to control plan is secured with the data and the qualities are secured in the customer's essential. This kind of approach is used for enormous business applications. How ever Property Based Encryption is furthermore used for data sharing and jointeffort works. Tu et al. [11] utilizes CPABE for outlining renouncement systems that permits fine grained get to control with high flexibility and renouncement.

Consider a specific undertaking application where a office allocates clients or individuals in a gathering with an arrangement of characteristics with their mystery key and conveys the mystery key to the separate clients. Any client that fulfills the get to control strategy characterized by the information partner can get to the information. At the point when a client disavows from the gathering, the get to rights to that information is expelled, and the information is re-encoded to make the denied client key futile. This technique is secured against picked figure content assaults against the CP-ABE demonstrate.

In any case, the plan is not exquisite on account of client repudiation since the upgrading of figure messages after client renouncement puts overwhelming calculation overhead.

Li et al. [11] use ABE with regards to the sharing of individual prosperity records (PHR) in the Cloud. Their structure includes an open range involving customers who make gets to on master records, for instance, pros, chaperons and remedial authorities, and moreover singular zone, which include customers who are before long related with the data proprietor, for instance, family and dear mates. Part attributes are dispensed to the customers in the all inclusive community range that addresses their master part and they recuperate their riddle keys from a quality expert. This is convincing as the data proprietor require not be online at all conditions. To the extent get the chance to control, data proprietors decide part based fine-grained get the chance to control approaches for their PHR archives. Using part based get to approaches uncommonly diminishes key organization overhead for proprietors and customers as the proprietor does not have to administer keys for each individual customer.

Middle Person Re-encryption

Middle person Re-encryption[15] is a champion among the most basic strategy for secured data sharing and composed exertion in the Cloud. It makes usage of semi-trusted mediator having re-mixed key to Convert a figure content mixed with

data proprietor or customer open key into other figure message that can be decoded by other customer's secret Key. The Plaintext won't be gotten to by the middle person. Pros use mediator re-encryption in context of cloud, for secure and private sharing of data. Consider an instance of data sharing amongst Alice and Bob, User Alice encodes his information D with an open key of her. When she needs to impart the information to Bob, Simply encoded information is sent to Intermediary and thusly the intermediary re-scrambles the encoded information with general society key of Bob. Presently Bob will have the capacity to decode the common information with the assistance of his Private key.

Intermediary Encryption with Data Sharing and Collaboration

Numerous analysts proposed Proxy re-encryption for secure what's more, classified information partaking in Cloud.

In [11],presented the idea of intermediary re-encryption strategy. In this strategy we generally accept that a predefined consents are alloted to the users.Here the private key of the information proprietor is softened up to two halfs ,where the primary portion of the key is put away at information proprietor's framework and the remaining part of the key is put away at Proxy Cloud. Whenever a client needs to get to the information and has the rights to get to it, information is decoded at intermediary once and with client's private key it is decoded second time to recover the first information. On the off chance that the proprietor of the information needs to repudiate a client from access to his information, he just educates to the intermediary cloud, then the intermediary evacuates the clients' half key. The fundamental favorable position of this procedure is ;

Hybrid ABE and Proxy Encryption

To gain more security and privacy for data sharing in cloud,we can use the combination of both Attribute Based Encryption(ABE) and Proxy Encryption(PE) techniques.Many researchers have focused on using the hybrid approach to provide robust and more trusted secure data sharing in cloud.

In [8] focussed on half breed approach by joining ABE,PE what's more, Lazy encryption systems for giving Security in cloud. In this system firstly an information proprietor encodes the plain content with symmetric key and after that the symmetric key is scrambled with the arrangement of traits as expressed in KP-ABE strategy. In this approach another client can participate to the gathering, the information proprietor doles out a get to structure and its mystery key is conveyed to the recently joined client. The information proprietor can deny a client by essentially recognizing an arrangement of qualities and upgrading its comparing access structure and the mystery key for the remaining clients is redesigned. The issue with this system is continuously the information proprietor ought to be online to give redesigned mystery keys. Be that as it may, the above procedure is robotized in the cloud by utilizing Proxy re-encryption approach which keeps the information secure and secret.

Another creator [10] additionally displayed to keep information sharing secure what's more, private by consolidating the cross breed approach ABE, PE. In this framework, information proprietor encodes the plain content with a arbitrary key say "k" and by utilizing access control approach called pol, he finds another arbitrary esteem 'k1'.Now 'k1'is scrambling utilizing ABE. He registers a key k2 by permitting operations on both k and k1 i.e k=k*k1.And then he scrambles this with his open key utilizing intermediary re-encryption. The keys are put away in cloud. The User with the required approval can get the intermediary key which is re-scrambled with the clients key. By this ABE key can be decoded and after that re computes k to unscramble the first document. The issue with this approach is the point at which a denied client rejoins a gathering with various approvals, yet he will have the capacity to recover the entrance to the past specified information which ought not be permitted.

Table 1: Survey on Secure and Confidentiality Data Sharing in Cloud

METHOD	ABE	PRE	Collision attack	User Revocation	Data Owner Online all the time
Scalable secure sharing [13]	Yes	No	No	Inefficient	No
Personal records sharing [14]	Yes	No	No	Efficient	No
Security in sharing data[15]	No	Yes	Yes	Efficient	No
Security & Privacy[8]	Yes	Yes	No	Inefficient	No
Secure and Confidential [16]	Yes	Yes	No	Efficient	No

III. DATA SHARING AMONG MULTIPLE OWNERS

One of the most important service offered by the cloud service providers is data storage. Let us Consider an exampleof data application. In a company or firm it allows a samegroup or department or team to store and share the files in thecloud. By using cloud, a company/staff will be away frommaintenance and trouble shooting of storage issues. Any how ithas privacy issues to the files stored in cloud. To protect theabsolutely free. Enjoy using this paraphrasing tool of ours and do spread the word!information from unapproved get to , we ought to scramble the information documents [11] before putting away into the cloud. Be that as it may, planning an productive information sharing plan for gatherings in the cloud have a few difficulties. To begin with issue, is, without the assurance of character protection, a client might be unwilling to participate in the cloud on account of effortlessly unveiling their genuine personalities to cloud suppliers and assailants. The Second issue is, it ought to bolster like multiple-information proprietor , that is any part in the gathering are permitted to appreciate the administrations information putting away and partaking in cloud. Last issue, gatherings ought to be alert in rehearse. To determine these difficulties, we introduce a protected multi-proprietor information sharing plan and the commitment of these paper :

- Any client or part in a gathering can safely share their information with others in an un trusted cloud [9].
- The proposed conspire likewise bolsters dynamic gatheringseffectively. In this way, recently allowed

clients can specifically unscramble the documents before reaching the information proprietors.

- Client disavowal likewise effortlessly accomplished. There is no compelling reason to redesign the mystery keys of the rest of the clients.
- We give secure and protection saving access control to clients. So any part in the gathering can secretly use the cloud asset and if any debate happens, then the amass director can uncover the genuine character of the comparing client. The few strategies are examined and there execution is appeared in the underneath Table 2.

A. Proposed Extensions for Multiple Owners

To address the some of the above issues and challenges,weproposed the following extensions for multiple owners across the groups in the Cloud computing scenarios.

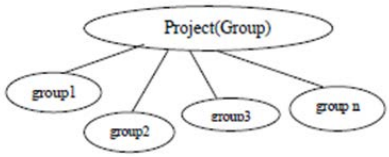

Fig. 1: Data Sharing Across Group Scenarios

These extensions will address the challenges in data Organization and security mechanisms such asencryption/ decryption with key management, and access privileges like read/write/update, among the multiple ownerswhich are spread across several groups in the system as depicted in Figure 1.

In the figure 1,the root node indicates group which is further classified into several sub groups. In each sub group there are multiple users who will be working on the data. for a single file, there could be multiple owners across the groups.

Table 2: Performanc Comparision

Method	Encryption Technique	Dynamic groups	Identity Privacy	Key Distribution	Revocation mechanism	Likelihood of Collusion attack
PLUTUS [3]	File - block key & lockbox-key	X	Satisfactory	Heavy	✓	X
SIRIUS[4]	Public key cryptography	X	Satisfactory	Heavy	✓	X
IMPROVED PROXY ENCRYPTION[5]	Proxy cryptography	✓	Less	Medium	✓	X
SECURE SCALABLE DATA ACCESS SCHEME [8]	KP-ABE technique	✓	Less	Depends upon number of revoked users	X	Y
MONA [18]	Broadcast encryption	✓	High	Independent of number of revoked users	✓	Y

For example, if the data generated at a point of time say X,could be belong to the many owners of the groups.

Groups are denoted by G, Users or members in the group are denoted by U,

where

G € $\{g_1,g_2,g_3,.....g_i\}$, $1 \le i \le n$ and n represents number of groups.

g_i€ $\{u_1,u_2,.....u_j\}$,where $1 \le j \le$ k and k represents the size of g_i

And data or file generated by a set of users in various groups represented by 'X'

X = { U12,U26,U31,...Uij}

here i € group and j € User or member in a group

B. Key Management

In distributed environments key management plays a major role for secure data access and efficient computation.

If key management is not properly done, then it leads to cloud unreliable. Hence it is necessary to much focus on key management for the cloud to provide for secure sharing of data in a group in cloud.

In the Traditional key management approach, each user in the group is given a specific key to access the data. This method is effective for less number of users in the group, but it does not scale up for large number of users and this is not cost effective. To overcome the above problem, our proposed system, uses a single key for each group instead of each particular user.

IV. CONCLUSION AND FUTURE ENHANCEMENT

In this paper we talked about a few security components in Mists for information sharing. We at first exhibited an overview on information sharing, get to, security and safeguarding instruments, taken after by one of the basic components in information sharing i.e. different proprietors information sharing issues. We have made crevice investigation in the information sharing, examined a model and augmentations required to address the numerous proprietors issues in the dynamic gatherings inside the Clouds. Advance our examination work incorporate tending to the difficulties in information association and security component over different proprietor for secure information sharing for various element bunches in cloud

A Future research heading is to keep up security and security, to store and process the information in cloud.

Right now the vast majority of the exploration work is centered around Data sharing and joint effort in the Cloud, illuminating client disavowal issues is still a testing issue where future research can be completed.

A potential research bearing is Auditing and Accountability in the Cloud with regards to information partaking in the Cloud. Since individuals from a gathering can complete illicit operations on the information. A future

research course is discover routes for information proprietor to consider responsible any part that does pernicious exercises on their information

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A.Patterson, A. Rabkin, I. Stoica and M.Zaharia, "A View of Cloud Computing", Comm. ACM, Vol. 53, No. 4, Pp. 50-58, 2010.

[2] D. Boneh and M. Franklin, "IdentityBasedEncryption from the Weil Pairing", Proc. Int'lCryptology Conf.Advances in Cryptology (CRYPTO), Pp.213-229, 2001.

[3] S. Yu, C. Wang, K. Ren and W. Lou,"Achieving secure, scalable and fine- grained data access control in cloud computing", Proc. OfINFOCOM, Pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang and K. Fu, "plutus: Scalable secure file sharing on untrusted storage", Proc. of FAST, Pp. 29-42, 2003.

[5] C. Wang, Q. Wang, K. Ren and W. Lou, "PrivacyPreserving Public Auditing for Data Storage Security in Cloud Computing", Proc. IEEE INFOCOM, Pp. 525-533, 2010.

[6] Q. Wang, C. Wang, J. Li, K. Ren and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing", Proc. 14th European Conf. Research in Computer Security (ESORICS09), Pp. 355- 370, 2009.

[7] D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps", Proc. EUROCRYPT., Pp. 416–432, 2003.

[8] R. Lu, X. Lin, X. Liang and X. Shen, "Secure Provenance: The Essential of Bread and Butter ofData Forensics in Cloud Computing", Proc. ACMSymp.Information, Computer and Comm Security, Pp. 282-292, 2010.

[9] B. Wang, B. Li and H. Li, "Knox: PrivacyPreserving Auditing for Shared Data with LargeGroups in the Cloud", 10th Int'l Conf.Applied Cryptography and Network Security, Pp.507-525, 2012.

[10] D. Artz and Y. Gil, "A Survey of Trust in Computer Science and the Semantic Web", J. Web Semantics: Science, Servicesand Agents on the World Wide Web, Vol. 5, No. 2, Pp. 58-71, 2007.

[11] L. Backstrom, D. Huttenlocher, J. Kleinberg and X. Lan, "Group formation in large social networks: membership, growth, and evolution", Proc. 12th international conference on Knowledge discovery and data mining, Pp. 44–54, 2006.