International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Utilizing a Secure Anti Collusion Mechanism for Dynamic Groups in order to Prevent the Data sharing collusion in the Cloud

Manjula T S[1], Manjunath k. G[2]

[1]*M.Tech Student, Dept. of Computer Science & Engineering, SIT, Tumakuru, Karnataka, India.*
[2]*Assistant Professor, Dept. of Computer Science & Engineering, SIT, Tumakuru, Karnataka, India.*

Abstract - *Profited from cloud computing, clients can accomplish a viable and efficient methodology for information sharing among gathering individuals in the cloud with the characters of low upkeep and little administration cost. Since the code will be outsourced, we provide a security measures for the sharing information documents. Lamentably, due to the incessant change of the enrollment, protecting the sharing information is a challenging task, particularly for an untrusted cloud because of the conspiracy assault. In addition, for existing plans, they use secure communication channels to provide the secured key distribution among the group, be that as it may, to have such channel is a solid presumption and is troublesome for practice. In this paper, we propose a safe information sharing plan for element individuals. To begin with, we propose a safe path for key appropriation with no safe correspondence channels, and the clients can safely get their private keys from gathering chief. Second, our plan can accomplish fine-grained access control, any client in the gathering can utilize the source in the cloud and repudiated clients can't get to the cloud again after they are denied. Third, we can secure the plan from intrigue assault, which implies that renounced clients can't get the first information record regardless of the possibility that they scheme with the untrusted cloud. In our methodology, by utilizing polynomial capacity, we can accomplish a protected client renouncement plan. At long last, our plan can accomplish fine proficiency, which implies past clients need not to overhaul their private keys for the circumstance either another client joins in the gathering or a client is disavowed from the gathering.*

Key Words: **Key distribution, Data Sharing, Access Control, Cloud Computing, Privacy Preserving**

1. INTRODUCTION

In cloud computing, cloud administration suppliers offer a deliberation of limitless storage room for customers to host information [4]. Cloud computing, with the attributes of characteristic information sharing and low support, gives a superior usage of assets. It can help customers diminish their money related overhead of information administrations by moving the neighborhood administrations framework into cloud servers.

To safeguard information protection, a typical methodology is to encode information records before the customers transfer the scrambled information into the cloud [5]. Be that as it may, security concerns turn into the principle imperative as we now outsource the capacity of information, which is conceivably touchy, to cloud suppliers. Lamentably, it is hard to plan a protected and effective information sharing.

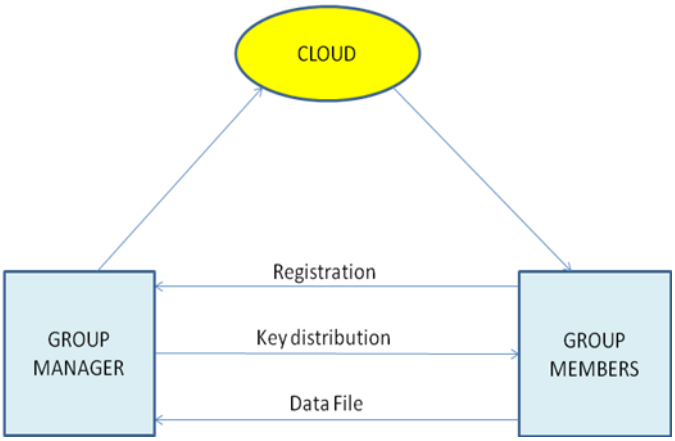

Fig-1: System Model

Fig. 1, the framework model comprises of three diverse elements: the cloud, a gathering chief and an extensive number of gathering individuals.

The cloud, kept up by the cloud administration suppliers, gives storage room to facilitating information documents in compensation as you- go way. Be that as it may, the cloud is untrusted since the cloud administration suppliers are effortlessly to end up untrusted. In this manner, the cloud will attempt to take in the substance of the put away information.

Group supervisor assumes responsibility of framework parameters era, client enlistment, and client denial. In the reasonable applications, the gathering supervisor as a rule is the pioneer of the gathering. In this manner, we accept that the gathering chief is completely trusted by alternate gatherings.

Group members (clients) are an arrangement of enlisted clients that will store their own particular information into the cloud and share them with others. In the plan, the

gathering enrollment is powerfully changed, because of the new client enlistment and client renouncement.

2. BACKGROUND

The cloud computing environment contains five qualities, three conveyance models and four organization models. The five vital qualities of cloud computing are including first stratum are: area free asset pooling that is supplier assets pooled to server various customers, on-interest self-administration, fast flexibility which is capacity to rapidly scale in/out administration, expansive system get to, and measured administration that is leasing the administrations use per pay premise.

1. Private cloud. The cloud infrastructure is operated solely for one organization. It may be managed by the organization or a third party and may exist on premise or off premise. Arguably this may be the most secure type of infrastructure, depending on the nature of the controls deployed and the diligence of the operator.

2. Community cloud. In this model, the cloud infrastructure could be shared by several organizations and supports a specific community or interest group that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

3. Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

4. Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Three Cloud Conveyance models are Iaas, PaaS and SaaS includes center stratum of cloud computing environment.

In Software as a Service (SaaS), applications are there that are empowered for the cloud. It underpins a design that can run various occasions of it-self which are area . This is only a month to month membership based estimating model and it is stateless. Examples of SaaS are MobileMe, Google docs, Zoho.

In Platform as Services, it incorporates stage on which engineers can compose their applications to be keep running on cloud environment. This stage typically has numerous application administrations accessible for speedy organization. Case of PaaS is Google Application Motor, Microsoft Sky blue, Force.com.

Infrastructure as a Service (IaaS) used by consumer by providing storage, processing, networking, and other fundamental computing resources where the consumer is able to deploy and run software, which can include operating systems and applications. It is highly scaled redundant and shared computing Infrastructure approachable using internet technologies. Examples of this type of delivery model include Amazon EC2, Sun's cloud services, Terremark cloud offering etc.

3. EXISTING METHODS

The author Kallahalla et al. [8] exhibited a cryptographic storage framework that empowers secure information sharing on conniving servers in light of the methods that isolating documents into record bunches and encoding every document bunch with a document square key. Not with standing, the document square keys should be redesigned and conveyed for a client denial; accordingly, the framework had a substantial key circulation overhead. Different plans for information sharing on untrusted servers have been proposed in [9] [10].In any case, the complexities of client support and repudiation in these plans are straightly expanding with the quantity of information proprietors and the denied clients.

Lu et al. [6] proposed a secure provenance scheme by leveraging group signatures and cipher text-policy attribute based encryption techniques [7]. Each user obtains two keys after the registration while the attribute key is used to decrypt the data which is encrypted by the attribute-based encryption and the group signature key is used for privacy preserving and traceability. However, the revocation is not supported in this scheme.

Liu et al. [3] introduced a protected multi-proprietor information sharing plan, named Mona. It is asserted that the plan can accomplish fine-grained access control and repudiated clients won't have the capacity to get to the sharing information again once they are revoked. Be that as it may, the plan will effortlessly experience the ill effects of the plot assault by the renounced client and the cloud [1]. The revoked client can utilize his private key to unscramble the scrambled information document and get the mystery information after his renouncement by contriving with the cloud. In the period of document access, most importantly, the denied client sends his solicitation to the cloud, then the cloud reacts the comparing encoded information record and revocation list to the renounced client without confirmations. Next, the denied client can figure the decoding key with the assistance of the assault calculation. At long last, this assault can prompt the repudiated clients getting the sharing information and uncovering different privileged insights of real individuals.

Nabeel et al. [2] proposed a protection safeguarding policy based content sharing plan in broad daylight mists. However, this plan is not secure in view of the frail insurance of responsibility in the period of character token issuance.

4. PROPOSED METHOD

In this paper, we propose a protected information sharing plan, which can accomplish secure key distribution and information sharing for element bunch. The primary commitments of our plan include:

We give a safe approach to key distribution without any safe correspondence channels. The clients can safely get their private keys from gathering administrator with no Certificate Powers due to the confirmation for people in general key of the client.

Our plan can accomplish fine-grained access control, with the assistance of the gathering client list, any client in the gathering can utilize the source in the cloud and revoked clients can't get to the cloud again after they are revoked.

We propose a protected information sharing plan which can be shielded from intrigue assault. The revoked clients can not have the capacity to get the first information documents once they are repudiated regardless of the fact that they plot with the untrusted cloud. Our plan can accomplish secure client repudiation with the assistance of polynomial capacity.

Our plan can bolster dynamic gatherings productively, when another client joins in the gathering or a client is denied from the gathering, the private keys of alternate clients don't should be recomputed and overhauled.

We give security investigation to demonstrate the security of our plan. Furthermore, we additionally perform reproductions to exhibit the productivity of our plan.

Data Owner (Group Member)
In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

Cloud Server
The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

Data Integrity
Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

Group Manager
The Group Manager who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data. The Group Manager will perform the revocation and un revocation of the remote user if he is the attacker or malicious user over the cloud data.

Data Consumer (End User / Group Member)
In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the GM authority and the Data users are controlled by the GM Authority only. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges.

5. EXPERIMENTAL RESULTS

In general, our proposed plan can accomplish secure key appropriation, fine get to control and secure client repudiation. For obviously seeing the upsides of security of our proposed plan, as represented in Table 1, we list a table contrasted and Mona, which is Liu et al's. plan, the RBAC plan, which is Zhou et al's. plan and ODBE plan, which is Delerablee et al's scheme. The √ in the clear means the plan can accomplish the comparing objective and also simulate in java platforms using an IDE Eclipse.

Security Performance Comparison

	Secure key distribution	Access control	Secure user revocation	Anti-collusion attack	Data confidentiality
Mona		√			
RBAC scheme		√			
ODBE		√	√	√	
Our scheme	√	√	√	√	√

Table 1: Security Performance Comparisons

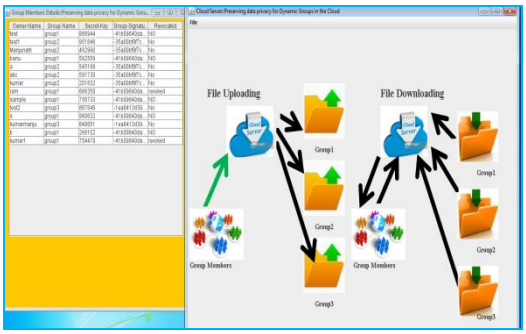

Fig-2: Sending group member details to cloud from group manager

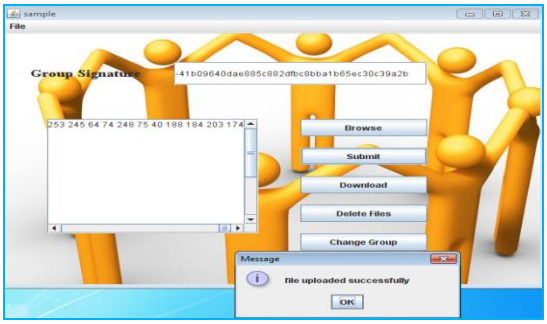

Fig-3: Replay message from cloud server when file is uploaded by group members

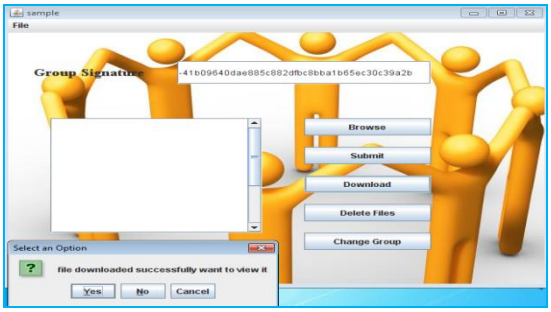

Fig-4: Replay message from cloud server when the file is downloaded

6. CONCLUSION AND FUTURE WORK

In this paper, we plan a safe hostile to intrigue information sharing plan for dynamic bunches in the cloud. In our plan, the clients can safely get their private keys from gathering director Declaration Powers and secure correspondence channels. Likewise, our plan can bolster dynamic gatherings proficiently, when another client joins in the gathering or a client is revoked from the group, the private keys of alternate clients don't should be recomputed and updated. In addition, our plan can accomplish secure client revocation, the revoked clients can not have the capacity to get the first information documents once they are revoked regardless of the possibility that they scheme with the untrusted cloud.

REFERENCES

[1] Z. Zhu, Z. Jiang, and R. Jiang, "The attack on mona: Secure multiowner data sharing for dynamic groups in the cloud," in Proc. Int.Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185–189.

[2] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602–2614, Nov. 2013.

[3] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans.Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[4] 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.

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

[6] 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. 282–292.

[7] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int.Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography,2008, pp. 53–70.

[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.