RESEARCH ARTICLE OPEN ACCESS

Data Security for Multi Users in Cloud by Using Cryptography Technique

S.Santhosh[1], K.MadhuBabu[2]
PG Student[1], M.Tech. Assistant Professor[2]
Department of Computer Science and Engineering,
Audisankara College of Engineering & Technology, Gudur.
AP-India

ABSTRACT

The major aims of this technique a secure multi-owner knowledge sharing theme. It implies that any user within the cluster will firmly share knowledge with others by the world organization trust worthy cloud. This theme is ready to support dynamic teams. Efficiently, specifically, new granted users will directly rewrite knowledge files uploaded before their participation whereas not contacting with knowledge owners. User revocation square measure just achieved through a very distinctive revocation list whereas not modification the key. Keys of the remaining users the size and computation overhead of cryptography square measure constant and freelance with the amount of revoked users. We've a bent to gift a secure and privacy-preserving access management to users that guarantee any member throughout a cluster to anonymously utilize the cloud resource. Moreover, the $64000 identities of information owners square measure disclosed by the cluster manager once disputes occur. We offer rigorous security analysis, and perform intensive simulations to demonstrate the potency of our theme in terms of storage and computation overhead. Cloud computing provides a cheap associated economical resolution for sharing cluster resource among cloud users sharing knowledge associate degree passing throughout a} terribly multi-owner manner whereas protecting knowledge Associate in Nursing identity privacy from an world organization responsible cloud continues to be a harissue, because of the frequent modification of the membership.

Keywords:- Multi owner, resource, cluster manager, revocation, Key Distribution

I. INTRODUCTION

CLOUD computing is recognized as another to ancient information technology as a result of its resource -sharing and low-maintenance characteristics. In cloud computing, the cloud service suppliers (CSPs), like Amazon, unit able to deliver various services to cloud users with the help of powerful data centres. By migrating the native data management systems into cloud servers, users can fancy high-quality services and save vital investments on their native infrastructures. One in every of the foremost basic services offered by cloud suppliers is data storage. Permit US to place confidence in a smart data application. A company permits its staffs inside identical cluster or department to store and share files inside the cloud. By utilizing the cloud, the staff's square measure typically totally discharged from the tough native data storage and maintenance. However, it in addition poses a significant risk to the confidentiality of these hold on files. Specifically, the cloud servers managed by cloud suppliers are not wholly trustworthy by users whereas the data files hold on inside the cloud may even be sensitive and confidential, like business plans. To preserve data privacy, a basic resolution is to jot down in code data files, and so transfer the encrypted data into the cloud [2].Sadly, planning degree economical and secure data sharing theme for teams inside the cloud is not an easy task as a result of the following issues. However, the complexities of user participation and revocation in these schemes square measure linearly increasing with the amount of information homeowners and so the vary of revoked users, severally. By setting a bunch with one attribute level projected a secure origin theme supported the cipher text-policy attribute-based cryptography technique, which allows any member throughout a cluster to share data with others. However, the matter of user revocation is not self-addressed in their theme conferred a scalable and fine-grained data access management theme in cloud computing supported the key policy attribute-based cryptography (KP-ABE) technique .Sadly, the one owner manner hinders the adoption of their theme into the case, where any user is granted to store and share data. Our contributions. To resolve the challenges conferred higher than, we've an inclination to propose Anglesey Island, a secure multi-owner data sharing theme for dynamic groups inside the cloud.

II. LITERATURE SURVEY

A. *Plutus: Scalable Secure File Sharing on Untrusted Storage*

Plutus may be a scientific discipline storage system that permits secure file sharing while not putting a lot of trust on the file servers. Specifically, it makes novel use of scientific discipline primitives to safeguard and share files. Plutus options extremely scalable key management whereas permitting individual users to retain direct management over United Nations agency gets access to their files. We have a tendency to make a case for the mechanisms in Plutus to scale back the quantity of scientific discipline keys changed between users by exploitation file groups, distinguish file scan and write access, handle user revocation expeditiously, and permit Associate in nursing untrusted server to authorize file writes. We've designed a epitome of Plutus on Open AFS. Measurements of this epitome show that Plutus achieves sturdy security with overhead such as systems that encrypt all network traffic.

B. *Sirius: Securing Remote Untrusted Storage*

This paper presents SiRiUS, a secure classification system designed to be superimposed over insecure network and P2P file systems like NFS, CIFS, OceanStore, and Yahoo! case. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptanalytic access management for file level sharing. Key management and revocation is easy with tokenish out-of-band communication. Classification system freshness guarantees square measure supported by SiRiUS mistreatment hash tree constructions. SiRiUS contains a completely unique technique of playing file random access during a cryptanalytic classification system while not the utilization of a block server. Extensions to SiRiUS embody giant scale cluster sharing mistreatment the NNL key revocation construction. Our implementation of SiRiUS performs well relative to the underlying classification system despite mistreatment cryptanalytic operations.

III. RELATED WORK

To preserve information privacy, a basic resolution is to encipher information files, then transfer the encrypted information into the cloud. sadly, coming up with associate degree economical and secure information sharing theme for teams within the cloud isn't a simple task.In the existing System information homeowners store the encrypted information files in untrusted storage and distribute the corresponding cryptography keys solely to approved users. Thus, unauthorized users moreover as storage servers cannot learn the content of the information files as a result of they need no data of the cryptography keys. However, the complexities of user participation and revocation in these schemes area unit linearly increasing with variety the amount the quantity of knowledge homeowners and also the number of revoked users, severally.

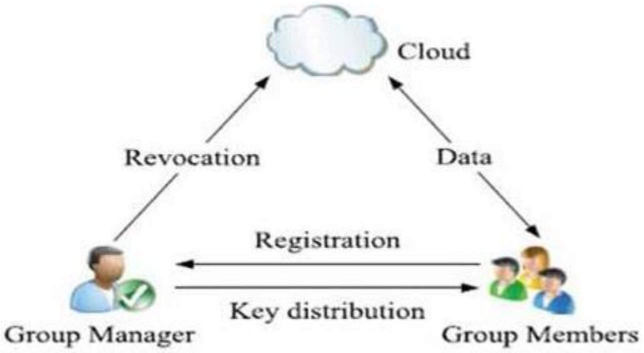

Fig1. Existing Model

1. In the prevailing Systems, identity privacy is one among the foremost vital obstacles for the wide preparation of cloud computing. While not the guarantee of identity privacy, users is also unwilling to affix in cloud computing systems as a result of their real identities may be simply disclosed to cloud suppliers and attackers. On the opposite hand, unconditional identity privacy might incur the abuse of privacy. for instance, a misbehaved employees will deceive others within the company by sharing false files while not being traceable.

2. Only the cluster manager will store and modify knowledge within the cloud.

3. The changes of membership create secure knowledge sharing extraordinarily troublesome the difficulty of user revocation isn't self-addressed.

IV. SYSTEM IMPLEMENTATION

1. We have an inclination to propose a secure multi-owner data sharing theme. It implies that any user inside the cluster can firmly share data with others by the world organisation sure cloud.

2. Our projected theme is during a position to support dynamic teams expeditiously. Specifically, new granted users will directly rewrite data files uploaded before their participation whereas not contacting with data

homeowners. User revocation is also merely achieved through a completely unique revocation list whereas not amendment the key keys of the remaining users. The size and computation overhead of cryptography square measure constant and freelance with the number of revoked users.

3. We provide secure and privacy-preserving access management to users that guarantees any member throughout a bunch to anonymously utilize the cloud resource. Moreover, the vital identities of information homeowners are also disclosed by the cluster manager once disputes occur.

4. We provide rigorous security analysis, and perform intensive simulations to demonstrate the potency of our theme in terms of storage and computation overhead.

.

A.Cloud section:

In this module, we tend to produce an area Cloud and supply priced torrential storage services. The users will transfer their information within the cloud. we tend to develop this module, wherever the cloud storage may be created secure. However, the cloud isn't absolutely trusty by users since the CSPs are terribly possible to be outside of the cloud users' trusty domain. kind of like we tend to assume that the cloud server is honest however curious. That is, the cloud server won't maliciously delete or modify user information owing to the protection of information auditing schemes, however can try and learn the content of the keep information and therefore the identities of cloud users.

B. Group Manager :

Group manager takes charge of followings
1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the important identity of a dispute knowledge owner.

Therefore, we tend to assume that the cluster manager is absolutely trustworthy by the opposite parties. The cluster manager is that the admin. The cluster manager has the logs of every and each method within the cloud. The cluster manager is accountable for user registration and additionally user revocation too.

C. Group Member :

1.store their non-public knowledge into the cloud server and

2.Share them with others within the cluster.
Note that, the cluster membership is dynamically modified, as a result of the workers resignation and new worker participation within the company. The cluster member has the possession of fixing the files within the cluster. Whoever within the cluster will read the files that are uploaded in their cluster and conjointly modify it.

D. File Security:

1. Encrypting the data file.
2. File stored in the cloud can be deleted by either the group manager or the data owner. (i.e., the member who uploaded the file into the server).

E. Group Signature :

A cluster signature theme permits any member of the group to sign messages whereas keeping the identity secret from verifiers. Besides, the selected cluster manager will reveal the identity of the signature's mastermind once a dispute happens, that is denoted as traceability.

F. User Revocation:

User revocation is performed by the cluster manager via a public out there revocation list (RL), supported that cluster members will cypher their information files and make sure the confidentiality against the revoked users.

G. Enhanced work

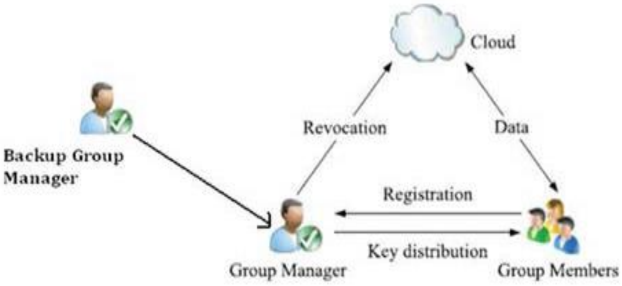

Fig 2.Proposed Model

In this strategy we are further showing how we are dealing with the dangers like disappointment of gathering chief by expanding the amount of reinforcement gathering supervisor, hanging of gathering director on the off chance that number of demands all the more by offering the workload in various gathering supervisors.

This strategy cases obliged effectiveness, versatility and above all dependability

To conquer the impediment of existing framework , in this proposed Scheme of data security is if the gathering director quit working because of expansive number of appeals originating from diverse gatherings of holders, then reinforcement bunch supervisor will stays accessible.

V. CONCLUSION

In this paper, we've an inclination to vogue a secure data sharing theme, for dynamic groups in associate world organisation trustworthy cloud. In Mona, a user is during a position to share data with others at intervals the cluster whereas not revealing identity privacy to the cloud. Additionally, Angle Sea Island supports economical user revocation and new user modification of integrity. lots of specially, economical user revocation are achieved through a public revocation list whereas not modification the private keys of the remaining users, and new users can directly decipher files keep at intervals the cloud before their participation. Moreover, the storage overhead and additionally the coding computation value are constant. Intensive analyses show that our projected theme satisfies the specified security requirements and guarantees efficiency additionally. Projected a science storage system that allows secure file sharing on world organisation trustworthy servers, named Plutus. By dividing files into file groups and encrypting each file cluster with a completely unique file-block key, the information owner can share the file groups with others through delivering the corresponding safe-deposit key, where the safe-deposit key's won't to write the file-block keys. However, it brings a few of significant key distribution overhead for large-scale file sharing. In addition, the file-block key should be updated and distributed yet again for a user revocation.

ACKNOWLEDGEMENT

This work was supported by K.MadhuBabu, M.Tech. Assistant Professor, Department of Computer Science and Engineering through his valuable guidance, constant encouragement, constructive criticism and keen interest.

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 ofCloudComputing," Comm. ACM, vol. 53,no. 4, pp. 50-58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, 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.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius:Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.

[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'lConf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001