Secure Data Sharing in Cloud Computing Using Revocable Storage Identity Based Encryption

1 G.Vijendar Reddy,Associate Professor,Dept of IT, Gokaraju Rangaraju Institute Of Engineering And Technology (Autonomous), Telangana,India gurramvijendarreddy@gmail.com
2 K.Varshith,Dept of IT,Gokaraju Rangaraju Institute Of Engineering And Technology (Autonomous), Telangana,India, varshith.k2001@gmail.com
3 B.Siva Mangaraju,Dept of IT,Gokaraju Rangaraju Institute Of Engineering And Technology (Autonomous), Telangana,India, sivamangarajuboramchu@gmail.com
4 S.Sahil, Dept of IT,Gokaraju Rangaraju Institute Of Engineering And Technology (Autonomous), Telangana,India, shaiksahil270@gmail.com
5 L.Harsha Vardhan,Dept of IT,Gokaraju Rangaraju Institute Of Engineering And Technology (Autonomous), Telangana,India, harshavardhan.lalam2001@gmail.com

ABSTRACT: Cloud computing offers a flexible and straightforward means of transferring data, which has numerous advantages for individuals and society as a whole. However, due to the fact that shared data frequently contains crucial information, consumers naturally hesitate to upload it directly to a cloud server. As a result, robust cryptographic data access control is required. Identity-based encryption provides a solid cryptographic foundation for the development of a useful data sharing system. Access control, on the other hand, is a moving target. There should be a process in place to remove users from the system when their authorisation expires so that they can no longer access the data. (RS - IBE) Revocable-storage identity-based encryption carries out this. We also demonstrate the security of a concrete RS-IBE building in the provided security model. The findings demonstrate the functional and efficiency benefits of the suggested RS-IBE strategy, enabling a workable and affordable data-sharing system. Finally, we provide the outcomes of the implementation to demonstrate the system's efficiency.

Keywords – *Cryptography, identity-based encryption, revocation, and cypher text.*

1. INTRODUCTION

A paradigm known as cloud computing offers enormous memory space and compute power at a cheap cost [1]. It provides customers with the ability to access desired services regardless of the time or place across many platforms (such as mobile devices and personal computers), which is quite convenient for cloud users. One of the many services that cloud computing provides is cloud storage, such as Amazon S3 [4], Microsoft Azure [2], and Apple's iCloud [2]. These services may offer a more adaptable and straightforward approach to data transfer over the Internet, which has numerous benefits for contemporary society [5, 6]. However, it is also subject to a number of security risks, which are the primary concerns of cloud customers [7]. First of all, entrusting customers' data to a cloud server implies that they have no control over it. Users could be hesitant since outsourced data often include sensitive and important information. Second, cloud servers are susceptible to attacks due to the adversarial nature of data exchange. Worse still, the cloud server itself might release user data for financial gain without authorization. Thirdly, data is exchanged in a dynamic manner. To put it

another way, once a user's authorization has expired, they should not be able to access data that has already been provided. To ensure that only users who are presently permitted may share the outsourced data, users wish to limit access to the data when outsourcing it to a cloud server.

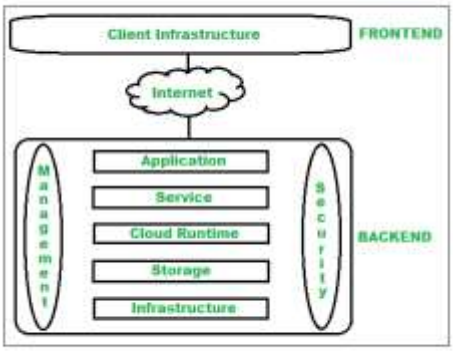

Fig.1: Example figure

Undoubtedly, such a data exchange mechanism may provide backward secrecy and confidentiality. The process of decrypting and re-encrypting all shared data can also guarantee forward secrecy. However, new challenges arise as a result. It should be noted that the decryption and re-encryption procedures necessitate the private key information of users, making the entire system for sharing data vulnerable to new attacks. The secret key should only be used for standard decryption and should not be used to regularly update the ciphertext. Efficiency presents a further obstacle. In order to update the ciphertext of the shared data, the data provider must perform the download, decrypt, reencrypt, and upload procedure on a regular basis. Due to the high connection and computation costs, this approach is burdensome and unfavorable for cloud customers with limited computing and storage capacity. Demanding that the cloud server explicitly re-encrypt the ciphertext of the shared data is one approach to resolving this issue. But this could lead to ciphertext extension, in which the amount of ciphertext for shared data grows linearly with update frequency. Additionally, the proxy re-encryption mechanism can be used to address the efficiency issue previously mentioned. Unfortunately, updating the ciphertext of the shared data also requires user interaction with the cloud server.

2. LITERATURE REVIEW

Social cloud computing: A vision for socially motivated resource sharing:

Usually Since certifiable ties are much of the time the groundwork of online collaborations in interpersonal organizations, deducing a level of trust between clients from these relationships is conceivable. We recommend utilizing these associations with make a dynamic "Social Cloud," permitting clients to trade

different assets inside the system of an informal organization. Likewise, by utilizing the inherent socially rectifying components (motivations, disincentives), a cloud-based system for long haul sharing might be made conceivable with less protection and security issues than ordinary cloud settings. It is recommended that a social commercial center be utilized as a method for controlling sharing in light of the unmistakable elements of the Social Cloud. The social market is one of a kind since it empowers exchange utilizing both social and financial shows. This article describes social cloud computing, discusses social clouds' different facets, and illustrates the methodology using Facebook's social storage cloud.

Privacypreserving public auditing for secure cloud storage:

With the assistance of cloud storage, clients may remotely store their information and take utilization of excellent applications and administrations on request from a common pool of reconfigurable registering assets without stressing over keeping up with and putting away their information locally. In any case, since clients never again truly hold the rethought information, safeguarding its trustworthiness in distributed computing is a difficult issue, especially for clients with restricted PC capacities. Also, clients most likely won't have to stress over really looking at the trustworthiness of the distributed storage; they ought to simply have the option to use maybe it were neighborhood. In this manner, it is essential to give public auditability to distributed storage with the goal that customers might use an third party auditor (TPA) to affirm the precision of reevaluated information and feel calm. The reviewing technique shouldn't make any new web-based loads for clients or weaknesses influencing client information protection to send a TPA securely and really. In this examination, we give a confidential public reviewing component for a solid distributed storage framework.We further expand our finding such that the TPA may effectively and concurrently conduct audits for a number of consumers. The suggested techniques are provably secure and very effective, according to a thorough investigation of security and performance.

An efficient and secure dynamic auditing protocol for data storage in cloud computing:

Users (information shoppers) may get to the information from cloud servers in distributed computing, where information proprietors have their information on cloud servers. Nonetheless, due to information rethinking, this new model of information facilitating administration additionally presents new security issues, requiring the utilization of a fair-minded evaluating administration to check the precision of the information in the cloud. Since the information in the cloud might be continually refreshed, certain ongoing distant uprightness checking procedures are restricted to static file material and can't be utilized for the examining administration. Hence, a dynamic evaluating convention that is viable and safe is expected to convince information proprietors that their information is being kept in the cloud properly. In this article, we first develop an examining structure for distributed storage frameworks and afterward set forward a useful evaluating convention that regards security. Then, since information dynamic activities are compelling and unquestionably protected in the arbitrary prophet worldview, we change our examining convention to

empower them. Without the guide of a dependable coordinator, we further grow our evaluating convention to oblige clump examining for both various proprietors and different mists. The examination and recreation discoveries show that our recommended evaluating techniques are compelling and secure, especially in bringing down the examiner's figuring costs.

Public auditing for shared data with efficient user revocation in the cloud:

Clients may rapidly change and divide information between themselves utilizing cloud-based information capacity and sharing administrations. Clients in the gathering should compute marks on each block of shared information to ensure that its trustworthiness can be autonomously approved by outsiders. Because of information refreshes made by numerous clients, separate blocks of shared information are ordinarily endorsed by different clients. The blocks that were recently endorsed by a client who has been taken out from the gathering should be re-endorsed by a current client for the sake of security. Because of the amount of shared information in the cloud, the straightforward technique — permitting a current client to download the applicable part of shared information and once again sign it upon client denial — is incapable. Considering powerful client renouncement, we give a one of a kind public reviewing framework for the respectability of shared information in this review. We make benefit of the idea of intermediary re-marks to empower the cloud to re-sign blocks for current clients after client disavowal, saving existing clients the difficulty of downloading and yet again sign blocks all alone. Moreover, regardless of whether a portion of the common material has been re-endorsed by the cloud, a public verifier may continuously take a look at the consistency of the information without downloading everything. Our system also supports batch auditing by concurrently checking several auditing jobs. Experimental findings indicate that our technique may greatly boost user revocation's effectiveness.

Decentralized access control with anonymous authentication of data stored in clouds:

For secure cloud data storage, we propose a novel decentralized access control system with anonymous authentication. According to the suggested plan, before saving data, the cloud authenticates the series without knowing who the user is. Our system also includes access control, which limits who may decrypt the stored data to authorised users. The system guards against replay attacks and allows for the production, alterations, and reading of cloud-stored data. We also talk about user termination. In contrast to previous access control methods made for clouds, which are centralised, our authentication and access control system is strong and decentralised. The overheads associated with communication, processing, and storage are equivalent to centralised methods.

3. METHODOLOGY

IBE was first put out for revocation by Boneh and Franklin. The key authority consistently gave non-repudiated clients private keys for each time span, and they annexed the ongoing time span to the ciphertext.

The suitable methodology were trailed by Boldyreva, Goyal, and Kumar to get the most ideal repudiation. Their RIBE procedure lessens the intricacy of key denial in the greatest number of framework clients to logarithmic, and they utilized a parallel tree to deal with distinguishing proof (as opposed to direct). Following that, Libert and Vergnaud proposed a powerfully safe RIBE framework in light of a changed variant of Water's IBE conspire utilizing the previously mentioned denial process.

Disadvantages:

- Why The ongoing innovation isn't versatile in light of the fact that it puts the essential weight of overseeing straight work as far as the quantity of non-disavowed clients. Besides, the dissemination of substitution keys by the vital power and clients who have not had their entrance denied requires a protected cycle.
- This sort of renouncement system can't avoid an intrigue between unfriendly non-disavowed clients and repudiated clients, in any event, when vindictive non-denied clients might share the update key with disavowed clients.
- The critical power of the plan should keep a table for every client to make the re-encryption key for each time span to refresh the ciphertext, which extraordinarily expands the weight of the key power.

Revocable identity based encryption (RIBE), which sticks to this way of thinking, is by all accounts a powerful strategy for maintaining the recently expressed security guidelines for information sharing.

- The RIBE framework has a structure that empowers a shipper to remember the ongoing span for the ciphertext, empowering The individual can decode it on the off chance that the beneficiary isn't renounced inside that time span.
- This system offers revocation, which allows users to access cloud-based files after receiving their password from the key authority. The data supplier has the option to stop allowing access to files. The customer won't log in again after that.

Advantages:

- We give a substantial design of RS-IBE that contains formal definitions for RS-IBE and the security model it is associated with.
- It can unquestionably provide both backward/forward security and secrecy at the same time.
- Only textual format types are acceptable in this project to convert data to an unintelligible format. It's probably accurate to claim that no identity-based encryption system before this one has ever been able to do this. It needs to use the revocable storage identity-based encryption method in order to create a far more affordable data sharing system (RSIBE).

Fig.2: System architecture

- The system's architecture, as shown above, outlines the general process and management. The three essential parts of this project are the key authority, user, data provider, and storage server.
- Data was first added to the cloud by data suppliers, who then made it accessible to users for viewing and retrieval. The secret key may be revoked and the data may be changed by the data source.
- At the point when a client needs to download a document, he sends a solicitation to the key Power, who then approves the user's data prior to sending the mystery key to the user. The key Authority manages keys for the system and manages keys between users and data providers.
- The system employs encryption when a data provider uploads data to the cloud to guarantee that when a nonuser tries to download the file, he gets encrypted data.

MODULES:

The following modules were created to carry out the aforementioned project.

- Key Authority(Auditor), Cloud User, Data Provider, and System Construction Module

MODULES DESCSRIPTION:

System Construction Module

In the main module, we foster the suggested philosophy with the important components for the evaluation of the recommended model. David, for instance, concludes who will share the data first (for instance, Alice and Bob). Then, utilizing the IDs Alice and Bob, David ensures that main approved clients transfer the scrambled message of the common information to the cloud server.

An unauthorised person or the cloud server cannot view the shared data's plaintext.

Data Provider

This module describes the Data Provider mode. New users must first register in the data provider system before signing in for authentication. The document might be transferred to the cloud server by utilizing the information supplier module. Safeguarding the most common way of bringing in information to the cloud

server includes utilizing a personality based design. The effectiveness of the file upload from the Data Provider will be assessed.

Cloud User

The Cloud User module is generated on this device. Before logging in to the Cloud user module for authorisation, new users must first register. The Cloud user may do a file search. Then, to get the file access request to the Auditor, the cloud user function is implemented. After receiving the decryption key from the auditor, the user may access the file. Once everything is done, the user logs out of the current session.

Key Authority (Auditor)

The Key Authority will visit the Key Authority page after logging in. The person will examine any open solicitations from the previously mentioned person. The individual will make an expert key for encryption and a mystery key for decoding subsequent to tolerating the previously mentioned individual's solicitation. The Auditor logs out of the session after the programme has done running.

4. EXPERIMENTAL RESULTS

Fig.3: Home screen

Fig.4: Registration

Fig.5: Auditor login page

Fig.6: upload data

Fig.7: User request

Fig.8: User request send for access

5. CONCLUSION

Cloud computing will be very advantageous to people. The rising growth of internet data interchange is mostly to blame. To make a financially savvy and secure information sharing framework in distributed computing, we made an idea called RS-IBE. This is finished by refreshing character disavowal and ciphertext simultaneously, which keeps denied clients from getting to information. The ideal RS-IBE method is demonstrated to be adaptively protected under the decisional l-DBHE supposition in this standard model, as well as a substantial RS-IBE development. The near discoveries exhibit that our technique performs better compared to the resistance as far as adequacy and value, making it more relevant for use in genuine settings.

6. FUTURE ENHANCEMENTS

In this project, we created all of the necessary conditions for secure data transfer. It is very challenging to get to the information without check in the cloud and we give denial techniques to erasing non-approved clients, and if by chance he did, the information would be in scrambled structure. We must do one thing in this model whenever the key authority views the user request and then sends the secret key to the user through email. Email is currently a highly effective application for sending data to others, therefore we must pay a premium to use this feature. This drawback may be able to be remedied by a feature.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: Towards a cloud definition,” ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2008.

[2] iCloud. (2014). Apple storage service [Online]. Available: https:// www.icloud.com/

[3] Azure. (2014). Azure storage service [Online]. Available: http:// www.windowsazure.com/

[4] Amazon. (2014). Amazon simple storage service (amazon s3) [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," IEEE Trans. Serv. Comput., vol. 5, no. 4, pp. 551–563, Oct.-Dec. 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[7] G. Anthes, "Security in the cloud," Commun. ACM, vol. 53, no. 11, pp. 16–18, 2010.

[8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[9] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92–106, Jan./Feb. 2015.

[10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 384–394, Feb. 2014.

[11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," IEEE Trans. Comput., vol. 64, no. 4, pp. 971–983, Apr. 2015, doi: 10.1109/TC.2014.2315619.

[12] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 468– 477, Feb. 2014.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. Adv. Cryptol., 1985, pp. 47–53.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

[15] S. Micali, "Efficient certificate revocation," Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. TM-542b, 1996.