International Journal of Science Engineering and Advance Technology

Efficient Cloud Storage Security Scheme and Data Sharing in Cloud

[1].CH. Veeraveni, [2]. K .V .V .L . Madhuri

[1.]final year student, MCA, Dept. of Computer science, IDEAL College of arts and sciences,Kakinada,AP, India
[2] .Assistant Proffeser Dept. of Computer Science, IDEAL College of art & science., vidyut nagar, kakinada, e.g.dt,AP, India.

ABSTRACT:
We propose the Secure Data Sharing in Clouds (SeDaSC) approach that gives: 1) information privacy and integrity; 2) get to control; 3) information sharing (sending) without utilizing register concentrated reencryption; 4) insider threat security; and 5) forward and in reverse access control. The SeDaSC strategy encodes a file with a solitary encryption key. Two distinctive key offers for every one of the clients are created, with the client just getting one offer. The ownership of a solitary offer of a key enables the SeDaSC system to counter the insider dangers. The other key offer is put away by a confided in outsider, which is known as the cryptographic server. The SeDaSC strategy is appropriate to traditional and portable cloud computing situations.

KEYWORDS: private keys, re-encryption, symmetric key.

1] INTRODUCTION:

Cloud computing is quickly rising because of the provisioning of mobile, adaptable, and on-request storage and figuring administrations for clients [1]. Associations with a low spending plan would now be able to use high registering and capacity administrations without vigorously putting resources into framework and upkeep [2]. Be that as it may, the loss of power over information and calculation raises numerous security worries for associations, ruining the wide flexibility of the open cloud. The loss of command over information and the capacity stage likewise rouses cloud clients to keep up the entrance authority over information (singular information and the information shared among a group of clients through the open cloud) [4]. Additionally, the protection and classification of the information is likewise prescribed to be thought about by the clients The secrecy the executives by a client guarantees that the cloud does not gain proficiency with any data about the client information. Cryptography is utilized as a commonplace instrument to give secrecy and security administrations to the information [5]. The information are generally scrambled before putting away to the cloud. The entrance control, key administration, encryption, and decoding forms are dealt with by the clients to guarantee information security [6].

2] LITERATURE SURVEY:

[1] S. Seo, We apply our mCL-PKE plan to build a down to earth answer for the issue of sharing touchy data in open mists. The cloud is utilized as a safe storage just as a key age focus. In our framework, the information owner encrypts the delicate information utilizing the cloud produced clients' open keys dependent on its entrance control strategies and transfers the encoded information to the cloud. Upon effective approval, the cloud somewhat unencrypts the scrambled information for the clients. The clients hence completely unscramble the in part decoded information utilizing their private keys. The secrecy of the substance and the keys is protected as for the cloud, on the grounds that the cloud can't completely decode the data. We additionally propose an augmentation to the above way to deal with improve the effectiveness of encryption at the information owner. We actualize our mCL-PKE conspire and the general cloud based framework, and assess its security and execution.

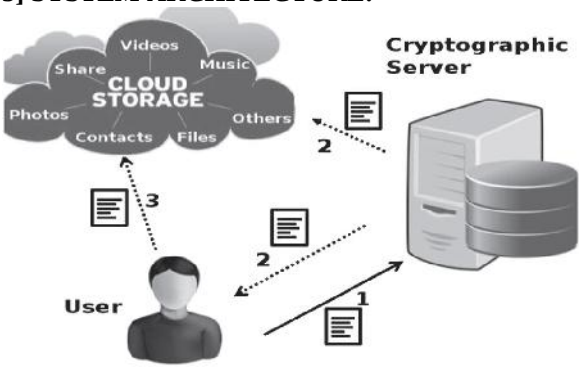
[2] Y. Chen, we propose a group key administration conspire dependent on a meta proxy re-encryption(PRE) plot. Specifically, we propose a RSA-based PRE plot with extraordinary properties. It is the first RSA-based PRE conspire for group key administration and has the ideal properties of uni-directionality and multi-bounce. In our group key administration plot, each group part holds only one mystery helper key and logN open assistant keys. The extent of rekey messages for each group key update remains O(logN). Moreover, our plan has some particular highlights. Right off the bat, the span of the key update history is a consistent O(N) regardless of how frequently of group key updates happen. Also, the calculation time of registering the freshest group key from the key update history is dependably O(logN) regardless of what number of group key

updates are missed. This component gives a reasonable answer for group key update when individuals go disconnected every now and then. At long last, the proposed plan is invulnerable to the agreement attack of different individuals.

4] PROPOSED APPROACH:

Accordingly, for every client in the gathering, the CS isolates the key into two sections with the end goal that a solitary part alone can't recover the key. Progressively, the first key is erased through secure overwriting. One piece of the key is transmitted to the comparing client in the gathering, though the other part is kept up by the CS inside the ACL identified with the information file. The ACL is created through the parameter presented by the information owner. The encoded information are therefore transferred to the cloud for capacity for the benefit of the client. The client who wishes to get to the information sends a download solicitation to the CS. The CS, in the wake of verifying the mentioning client, gets the segment of the key from the client and in this manner downloads the information file from the cloud.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

Cloud:

The cloud provides storage services to the user. The data on the cloud need to be secured against privacy breaches. The confidentiality of the data is ensured by storing encrypted data over the cloud. The cloud in the SeDaSC methodology only involves basic cloud operations of file upload and download. Therefore, no changes at the protocol or implementation
level on the cloud are required.

Cryptographic Server:

The CS is a trusted party and is responsible for security operations, such as keymanagement, encryption, decryption, the
management of the ACL for providing confidentiality, and secure data forwarding among the group. The users of SeDaSC are
required to be registered with the CS to obtain the security services. The CS is assumed to be a secure entity in the proposed methodology. The CS can be maintained by an organization or can be owned by a third-party provider. However, the CS maintained by an organization will generate more trust in the system.

Users:

The users are the clients of the storage cloud. For each data file, one user will be the owner of the file, whereas the others in the group will be the data consumers. The owner of the file decides the access rights of the other group members. The access rights are granted and revoked based on the decision of the owner. The access rights are managed by the CS in the form of an ACL file. A separate ACL is maintained for each of the data files.

ALGORITHM:

EFFICIENT CLOUD STORAGE SECURITY SCHEME AND DATA SHARING IN CLOUD

INPUT: DO, U, ACL, F, CS, CLOUD

Step1: owner of the file sends the encryption request to the CS.

Step2: list is sent to the CS only if the data are to be shared with a new proposed group.

Step3: encrypt the file and the CS generates *Ki* and *K* for every user and deletes *K* by secure overwriting.

Step4: The authorized user sends a download request to the CS.

Step5: downloads the encrypted file from the cloud and sends the decryption request to the CS.

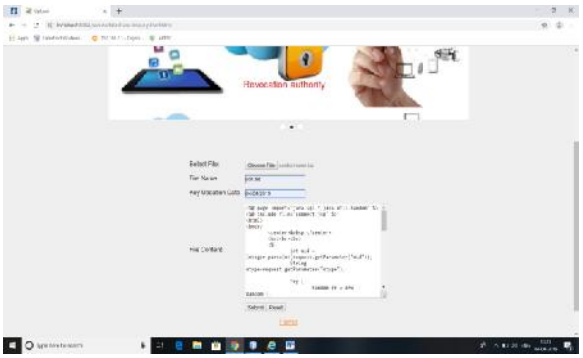
Step6: cloud verifies the authorization of the user through a locally maintained ACL.

Step7: the correct key *i* is received by the CS, the result will be a successful decryption.

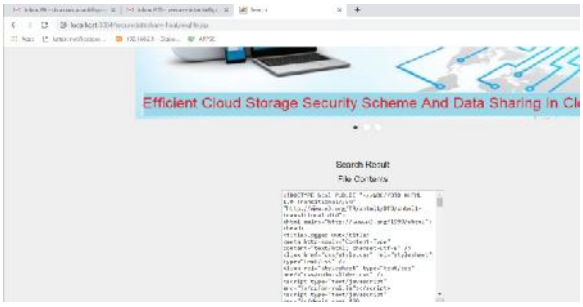
Step8: otherwise, the decryption will fail.

8] RESULTS:

OWNER UPLOAD THE FILE



USER DOWNLOAD THE FILE



9] CONCLUSION:

We proposed the SeDaSC approach, which is a cloud storage security conspire for group information. The proposed procedure gives information secrecy, secure information sharing without reencryption, get to control for pernicious insiders, and forward and in reverse access control. In addition, the SeDaSC technique gives guaranteed cancellation by erasing the parameters required to unscramble a document. The encryption and unscrambling functionalities are performed at the CS that is a confided in outsider in the SeDaSC system. The proposed methodology can be also employed to mobile cloud computing due to the fact that compute-intensive tasks are performed at the CS. The working of SeDaSC was formally analyzed using HLPNs, the SMT-Lib, and a Z3 solver. The performance of the SeDaSC methodology was evaluated based on the time consumption during the key generation, file upload, and file download operations.

10] REFERENCES:

[1] A. Abbas and S. U. Khan, "A review on the State-of-the-art privacy preserving approaches in e-health clouds," IEEE J. Biomed. Health Informat., vol. 18, no. 1, pp. 1431–1441, Jul. 2014.

[2] K. Alhamazani et al., "An overview of the commercial cloud monitoring tools: Research dimensions, design issues, state-of-the-art," Computing, DOI: 10.1007/s00607-014-0398-5, 2014, to be published.

[3] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," Future Gen. Comput. Syst., vol. 29, no. 5, pp. 1278–1299, Jul. 2013.

[4] L. Wei, H. Zhu, Z. Cao, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Inf. Sci., vol. 258, pp. 371–386, Feb. 2014.

[5] Cloud security Alliance, "Security guidelines for critical areas of focus in cloud computing v3.0," 2011.

[6] D. Chen et al., "Fast and scalable multi-way analysis of massive neural data," IEEE Trans. Comput., DOI: 10.1109/TC.2013.2295806, 2014, to be published.

[7] A. N. Khan, M. M. Kiah, S. A. Madani, M. Ali, and S. Shamshir-band, "Incremental proxy re-encryption scheme for mobile cloud computing environment," J. Supercomput., vol. 68, no. 2, pp. 624–651, May 2014.

[8] Y. Chen and W. Tzeng, "Efficient and provably-secure group key management scheme using key derivation," in Proc. IEEE 11th Int. Conf. TrustCom, 2012, pp. 295–302.

[9] L. Xu, X. Wu, and X. Zhang, "CL-PRE: A certificateless proxy reencryption scheme for secure data sharing with public cloud," in Proc. 7th ACM Symp. Inf. , Comput. Commun. Security, 2012, pp. 87–88.

[10] P. Gutmann, "Secure deletion of data from magnetic and solid-state memory," in Proc. 6th USENIX Security Symp. Focusing Appl. Cryptography, 1996, p. 8.

[11] S. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," IEEE Trans. Knowl. Data Eng., vol. 26, no. 9, pp. 2107–2119, Sep. 2013.

[12] Y. Chen, J. D. Tygar, andW. Tzeng, "Secure group key management using uni-directional proxy re-encryption schemes," in Proc. IEEE INFOCOM, pp. 1952–1960.

[13] T. Murata, "Petri Nets: Properties, analysis and applications," Proc. IEEE, vol. 77, no. 4, pp. 541–580, Apr. 1989.

[14] L. Moura and N. Bjrner, "Satisfiability modulo theories: An appetizer," in Proc. Formal Methods, Found. Appl., vol. 5902, Lecture Notes in Computer Science, 2009, pp. 23–36.

[15] S. U. R. Malik, S. K. Srinivasan, S. U. Khan, and L. Wang, "A methodology for OSPF routing protocol verification," in Proc. 12th Int. Conf. ScalCom, Changzhou, China, Dec. 2012, pp. 1–5.

CH.VEERAVENI is a student of P G Department of computer science in IDEAL College of Art & Sciences, Kakinada. Presently she is in final year MASTER COMPUTER APPLICATION (MCA) in this college and affiliated to Adikavi Nanaya University, Rajamahendravaram, Andhra Pradesh. She received her B.Sc (CS) from ADITYA DEGREE COLLEGE FOR WOMENS, Kakinada in the year 2016.Her area of interests include Data mining and Web designing all current trends and techniques in computer science.

MS K.V.V.L MADHRI is presently working as Assistant Professor in P.G Department of Computer science, Ideal college of Arts & sciences, Kakinada. She obtained her M.Sc in computer science from Andhra University. Her areas of interest include Software Engineering, Data base management system, Computer networks etc.