A Security Based Key Update File Sharing In Groups with Revoke Users in Cloud

MALA MAHESH KUMAR[1], DR.C.MD.GULZAR[2]
[1] PG Scholar, Dept of CSE, Dr. K. V. Subba Reddy Institute of Technology, Kurnool, AP, India.
[2]Professor & HOD, Dept of CSE, Dr. K. V. Subba Reddy Institute of Technology, Kurnool, AP, India.

ABSTRACT

Cyber Defense shows that the depth of resistance is always important for the protection of applications; it is a big problem for many applications. Recently, to deal with the problem of cloud storage, audit setting and significant proposed study. Challenges, to cope with the current solution for mobile phones, especially when the customer will essentially be able to calculate such resources, bring them to the customer who will be updated with the new position of load of their secret essential key. The period of time is limited, as is. In this paper, we will be able to offer a new paradigm focus on cloud storage as possible to outsourcing customer and key updates, key updates to transparent audit. In this paradigm, it is important, then you can be efficient out of the safe party, and important updates to customer load will be minimized. TPA with our design, all legal actions of the customer, the customer is required to hold an encrypted version of a secret key. TPA

secret key from encrypted download, upload new files to cloud client. In addition, the Validity of our design to verify the encrypted secret key is fitted to customers with the ability to deliver TPA. Transparent resistance as possible with important performance features of the audit process, carefully designed tomake the customer. We include a formal security model definition and parameters. Safety instantiations that display on our detailed design and simulation shows are safe and effective performance. We further extended the system by adding concept group file sharing with read, write permissions, and revoke user concept

I.INTRODUCTION

Distributed computing, as another innovation worldview with promising further, is turning out to be increasingly prominent these days. It can furnish clients with apparently boundless figuring asset. Endeavors and individuals can outsource tedious calculation workloads to cloud without spending the additional capital on conveying and keeping up equipment and programming. In momentum years, outsourcing calculation has included much consideration and been examined broadly. It has been considered in numerous applications including exploratory calculations direct arithmetical calculations straight programming calculations and secluded exponentiation calculations and so forth. In addition, distributed computing can likewise furnish clients with evidently boundless capacity asset. Distributed storage is all around saw as a standout amongst the most critical administrations of distributed computing. Despite the fact that distributed storage gives huge advantage to clients, it brings new security testing issues. One critical security issue is the means by which to effectively check the honesty of the information put away in cloud. In cutting edge years, numerous evaluating conventions utilized for distributed storage have been proposed to manage this issue. These conventions concentrate on various parts of distributed storage examining,

For example, the high proficiency the security assurance of information the security insurance of personalities element information operations the information sharing and so on. The key presentation issue, as another imperative issue in distributed storage reviewing, has been considered as of late. The inconvenience itself is no paltry by nature. Once the customer's mystery key for capacity inspecting is appearing to cloud, the cloud can basically conceal the information misfortune occurrences for keeping up its notoriety, even dispose of the customer's information once in a while got to for sparing the storage room. Yu et al. built a distributed storage inspecting convention with key-introduction strength by redesigning the client's mystery key occasionally. Along these lines, the harm of key presentation in distributed storage reviewing can be lessened. Be that as it may, it likewise gets new neighborhood loads for the customer in light of the fact that the customer needs to execute the key upgrade calculation in each day and age to make his mystery key push ahead. For a few customers with constrained calculation assets, this paper dislikes doing such additional calculations independent from anyone else in every day and age. It would be clearly better-hoping to make key upgrades as straightforward as could be expected under the circumstances for the customer, particularly in continuous key overhaul situations.

In this record, it considers accomplishing this objective by outsourcing key overhauls.Not with standing, it needs to fulfill a few new prerequisites to accomplish this objective. Firstly, the genuine customer's mystery keys for distributed storage review ought not to be known by the approved party who performs outsourcing calculation for key overhauls. Else, it will bring the new security risk. So the approved party ought to just hold an encoded form of the client's mystery key for distributed storage evaluating. Also, in light of the fact that the approved party performing outsourcing calculation just knows the encoded mystery keys, key upgrades ought to be finished under the scrambled state. In different terms, this approved gathering ought to be able to overhaul mystery keys for distributed storage examining from the scrambled variant he holds. Thirdly, it ought to be particularly effective for the customer to recuperate the verifiable mystery key from the encoded variant that is recovered from the approved party. In conclusion, the customer ought to have the capacity to check the legitimacy of the scrambled mystery key after the customer recovers it from the approved party. The objective of this paper is to outline a distributed storage evaluating convention that can fulfill above prerequisites to accomplish the outsourcing of key redesigns. We further extended the system by adding concept group file sharing with read and write permissions and revoke user concept

II.RELATED WORK

Outsourcing Computation: Time consuming computations has become a hot topic in the researchof the theoretical computer science in the recent two decades. Outsourcing computation has beenconsidered in many application domains [4].A new paradigm called cloud storage auditing system is proposed. In this new technique the key client operation is not performed by the client.The key update operation is performed by the authorized party. The authorized party holds the encrypted secret key of the client for client for cloud storage auditing.[8] The client downloads the encrypted secret key from the authorized party and decrypt it only when the client need to upload any new files to cloud. The client needs to check the validity of the encrypted secret key. The secret keys for cloud storage auditing are updated periodically.[4] As a result, any dishonest behaviors, such as deleting or modifying the client's data previously stored in cloud, can all be detected, even if the cloud gets theclient's current secret key for cloud storage auditing. However, the client needs to update his secret key ineach time period.Existing solutions all require the client to update the secret keys in every time period which mayinevitably bring in new local burdens to the client especially those with limited computation resources. The client is the owner of the files that are uploaded to cloud. The total size of these files is not fixed that is the client can upload the growing files to cloud in different time points. The cloud stores the client'sfiles and provides download service for the client. Important security problem is how to efficiently check the integrity of the data stored in storage area. With limited computation resources the users might notlike doing such extra computations by themselves in each time period.

III PROBLEM STATEMENT

The key exposure problem, as another important problem in cloud storage auditing, has been considered recently. The problem itself is non-trivial by nature. Once the client's secret key for storage auditing is exposed to cloud, the cloud is able to easily hide the data loss incidents for maintaining its reputation, even discard the client's data rarely accessed for saving the storage space.

IV.IMPLEMENTATION

We propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this new paradigm, key-update operations are not performed by the client, but by an authorized party. The authorized party holds an encrypted secret key of the client for cloud storage auditing and updates it under the encrypted state in each time period. The client downloads the encrypted secret key from the authorized party and decrypts it only when he would like to upload new files to cloud. In addition, the client can verify the validity of the encrypted secret key. We design the first cloud storage auditing protocol with verifiable outsourcing of key updates. In our design, the third party auditor (TPA) plays the role of the authorized party who is in charge of key updates. In addition, similar to traditional public auditing protocols, another important task of the TPA is to check the integrity of the client's files stored in cloud. The TPA does not know the real secret key of the client for cloud storage auditing, but only holds an encrypted version. In the detailed protocol, we use the blinding technique with homomorphic property to form the encryption algorithm to encrypt the secret keys held by the TPA. It makes our protocol secure and the decryption operation efficient. Meanwhile, the TPA can complete key updates under the encrypted state. The client can verify the validity of the encrypted secret key when he retrieves it from the TPA. In this protocol, key updates are outsourced to the TPA and are transparent for the client. The TPA only sees the encrypted version of the client's secret key, while the client can further verify the validity of the encrypted secret keys when downloading them from the TPA. We further extended the system by adding concept group file sharing with read and write permissions and revoke user concept

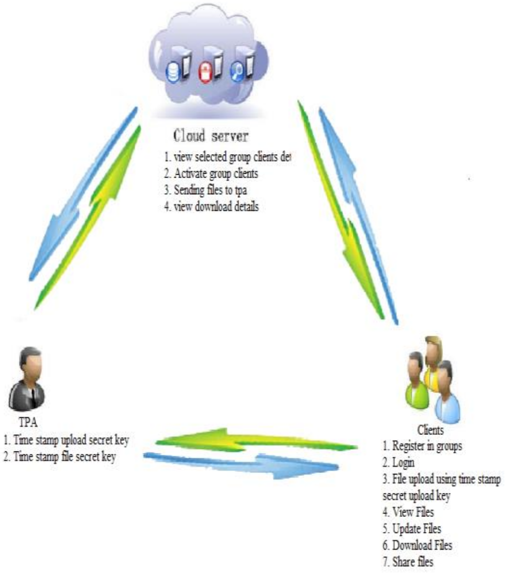
Cloud server
1. view selected group clients det
2. Activate group clients
3. Sending files to tpa
4. view download details
TPA
1. Time stamp upload secret key
2. Time stamp file secret key
Clients
1. Register in groups
2. Login
3. File upload using time stamp secret upload key
4. View Files
5. Update Files
6. Download Files
7. Share files

Figure: System Architecture

V.MODULES DESCRIPTION

1. Client Module.

2. Time Stamp Upload Key Module

3. Time Stamp File Key Module

4. Third Party Auditor(TPA) Module

5. Cloud Module

1. Client Module

This module includes the Client registration and client login details. Every Client need to register while accessing to the cloud. Every Client will be activated by the Cloud. After Cloud activated, every Client need to provide time stamp upload key to upload a new files into cloud. Time stamp upload key will be provided by third party auditor. Client need to download the time stamp upload key when client uploading new files into cloud. Client can view file details and download the file using time stamp file key provided by TPA.

2. Time stamp upload key:

Time stamp upload key will be provided by TPA. Client can download the upload key each time client uploading new file into cloud and they need not to give request key from TPA. At the time of client downloading the time stamp upload key, the request will send in directly to TPA and update according to time by TPA and send encrypted upload secret key to client. And finally, client can decrypt download the upload secret key. After getting decrypt upload secret key, now Client can upload a new file into cloud.

3. Time stamp file key:

Each time client accessing and downloading the file from cloud, TPA will provide each time file update key to client registered mail Id. So same file key will not be there for same file. It will send as file time stamp update key, so corresponding client can use this file from different server without any other use of hacker or attacker. If Client again login with same server or different server, same file key will not been used by Client to download the file for more security.

4. Third Party Auditor (TPA) Module

It acts as admin. TPA Provide time Upload secret key in Encrypted state for every client to upload new file into cloud. It will be send as in directly while Client downloading the upload key. The upload secret key, while user downloading key it will updated according to time. After cloud given auditing proof then only TPA can audit all files. And also provide the File Stamp key for all files to the client request for corresponding files key.

5. Cloud Module

Activate data client. Cloud sends storage auditing proof for all files to TPA. Cloud can view the client downloaded files from cloud.

VI.CONCLUSION

we study on how to outsource key updates for cloud storage auditing with key-exposure resilience. We propose the first cloud storage auditing protocol with verifiable outsourcing of key updates. In this protocol, key updates are outsourced to the TPA and are transparent for the client. In addition, the TPA only sees the encrypted version of the client's secret key, while the client can further verify the validity of the encrypted secret keys when downloading them from the TPA. We give the formal security proof and the performance simulation of the proposed scheme. We further extended the system by adding concept group file sharing with read and write permissions and revoke user concept.

VII. REFERENCES

[1] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientificcomputations," Adv. Comput., vol. 54, pp. 215–272, 2002.

[2] D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic computations," in Proc. 6th Annu. Conf. Privacy, Secur. Trust, 2008, pp. 240–245.

[3] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE INFOCOM, Apr. 2011, pp. 820–828.

[4] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Secur., 2012, pp. 541–556.

[5] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[6] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[7] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology. Berlin,Germany: Springer-Verlag, 2008, pp. 90–107.

[8] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable datapossession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, Art. ID 9.

[9] F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol.20, no. 8, pp. 1034–1038, Aug. 2008.

[10] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiplereplica provable data possession," in Proc. 28th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2008, pp. 411–420.

[11] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Efficient provable data possession for hybrid clouds," in Proc. 17th ACM Conf. Comput. Commun.Secur., 2010, pp. 756–758.

[12] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," IEEE Netw., vol. 24, no. 4, pp. 19–24, Jul./Aug. 2010.

[13] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics forstorage security in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859,

May 2011.

[14] K. Yang and X. Jia, "Data storage auditing service in cloud computing: Challenges, methods andopportunities," World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.

[15] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced

storages in clouds," IEEE Trans. Services Comput., vol. 6, no. 2, pp. 227–238, Apr./Jun. 2013.

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