© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

Dynamic and Public Auditing with Fair Arbitration for Cloud Data

Amit Kumar Pandey
Kopal Institute of Science & Technology
CSE,Bhopal (M.P)

Prof. Nitin Choudhary
Kopal Institute of Science & Technology
CSE,Bhopal (M.P)

ABSTARCT: Cloud users no longer physically hold their data, so how to protect the nobility of their outsourced data becomes a challenging task. In Cloud, privacy protection of data is also an important feature of cloud storage auditing. In order to lower the computational load of the client, a third-party auditor (TPA) is introduced to help the client to periodically check the integrity of the data in cloud. it is feasible for the TPA to get the client's data after it executes the auditing protocol multiple times. Auditing protocols are designed to ensure the privacy of the client's data in cloud. Another aspect having been addressed in cloud storage auditing is how to support data dynamic operations. I have proposed an auditing protocol supporting fully dynamic data operations including modification, insertion and deletion.

KEYWORDS: Encryption algorithm; Dynamic Auditing; Data integrity; Fairness Protocol

ISSN : 2278-6848
03
9 772278 684800
© International Journal for
Research Publication and Seminar

1. INTRODUCTION

Information or Data outsourcing is a key use of distributed computing, which pacify cloud clients of the solid weight of information administration and framework support, and gives fast information get to autonomous of physical areas. Cloud storage auditing is used to verify the integrity of the data stored in public cloud, which is one of the important security techniques in cloud storage. In recent years, auditing protocols for cloud storage have attracted much observation and have been researched intensively. These protocols focus on several different aspects of auditing, and how to achieve high bandwidth and computation efficiency is one of the essential concerns. For that purpose, the Homomorphism Linear Authenticator (HLA) technique that supports block less verification is explored to reduce the overheads of computation and communication in auditing protocols, which allows the auditor to verify the integrity of the data in cloud without recover the whole data. Many cloud storage auditing protocols like have been proposed based on this technique. The privacy protection of data is also an important aspect of cloud storage auditing. In order to lower the computational burden of the client, a third-party auditor (TPA) is introduced to help the client to periodically check the integrity of the data in cloud. However, it is possible for the TPA to

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

get the client's data after it executes the auditing protocol multiple times. Auditing protocols are designed to protect the privacy of the client's data in cloud. Another aspect

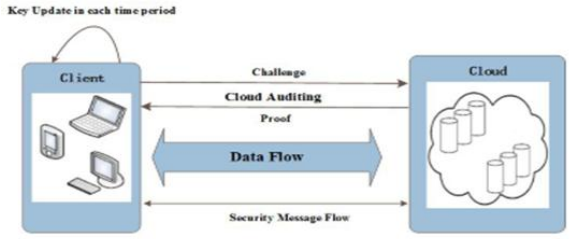


Fig: 1 System Model of Cloud Storage

2. PROBLEM STATEMENT

Though many research works about cloud storage auditing have been done in recent years, a critical security problem the key exposure problem for cloud storage auditing, has remained unexplored in previous researches. While all existing protocols focus on the faults or dishonesty of the cloud, they have overlooked the possible weak sense of security and/or low security settings at the client. Unfortunately, previous auditing protocols did not consider this critical issue of how to deal with the client's secret key exposure for cloud storage auditing, and any exposure of the client's secret auditing key would make most of the existing auditing protocols unable to work correctly. Cloud Computing has come into reality as a new IT infrastructure built on top of a series of techniques such as distributed computing, virtualization, etc. Besides the many benefits that it can bring forth, Cloud Computing also introduces the difficulty of protecting the security of data outsourced by cloud users.

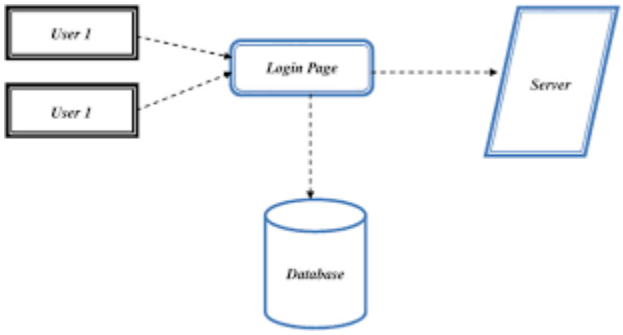
having been addressed in cloud storage auditing is how to support data dynamic operations.

Auditing protocols can also support dynamic data operations. Other aspects, such as proxy auditing, user revocation and eliminating certificate management in cloud storage auditing have also been studied. We focus on how to reduce the damage of the client's key exposure in cloud storage auditing. Our goal is to design a cloud storage auditing protocol with built-in key-exposure resilience. How to do it efficiently under this new problem setting brings in many new challenges to be addressed below.

First of all, applying the traditional solution of key revocation to cloud storage auditing is not practical. This is because, whenever the client's secret key for auditing is exposed, the client needs to produce a new pair of public key and secret key and regenerate the authenticators for the client's data previously stored in cloud. The process involves the downloading of whole data from the cloud, producing new authenticators, and re-uploading everything back to the cloud, all of which can be tedious and clumsy. Besides, it cannot always guarantee that the cloud provides real data when the client regenerates new authenticators. Secondly, directly adopting standard key-evolving technique is also not suitable for the new problem setting. It can lead to retrieving all of the actual files blocks when the verification is preceded. This is partly because the technique is incompatible with block less verification.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

The resulting authenticators cannot be aggregated, leading to unacceptably high computation and communication cost for the storage auditing.



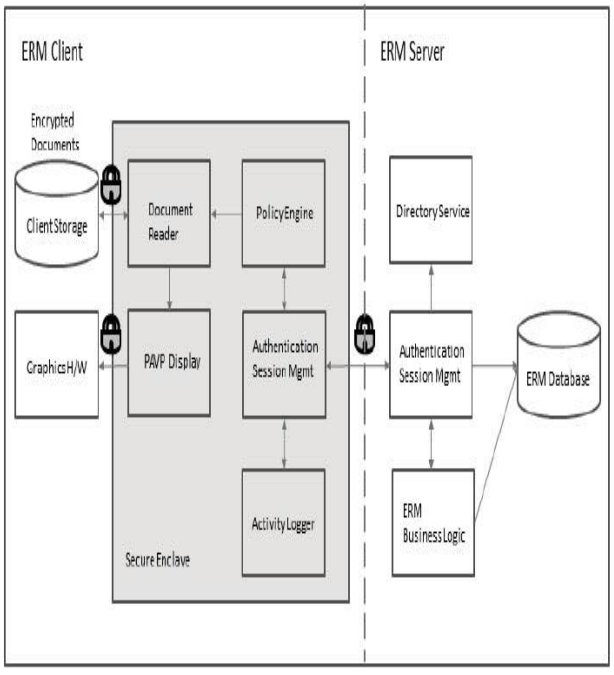


Fig2: Process Flow Diagrams for Existing and Proposed System

In this paper, we focus on how to reduce the damage of the clients' key exposure in cloud storage auditing. Our goal is to design a cloud storage auditing protocol with built-in

3. PRPOSED WORK

key-exposure resilience. How to do it efficiently under this new problem setting brings in many new challenges to be addressed below. First of all, applying the traditional solution of key revocation to cloud storage auditing is not practical. This is because, whenever the client's secret key for auditing is exposed, the client needs to produce a new pair of public key and secret key and regenerate the authenticators for the client's data previously stored in cloud.

Our goal is to design a practical auditing protocol with key-exposure resilience, in which the operational complexities of key size, computation overhead and communication overhead should be at most sub-linear to T. In order to achieve our goal, we use a binary tree structure to appoint time periods and associate periods with tree nodes by the pre-order traversal technique. The secret key in each time period is organized as a stack. In each time period, the secret key is updated by a forward-secure technique.

The auditing protocol achieves key-exposure resilience while satisfying our efficiency requirements. As we will show later, in our protocol, the client can audit the integrity of the cloud data still in aggregated manner, i.e., without retrieving the entire data from the cloud.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

Fig 3: Implementation of Proposed Work

4. CONCLUSION & FUTURE WORK

In this paper we study on how to deal with the client's key exposure in cloud storage auditing. We propose a new paradigm called auditing protocol with key-exposure resilience. In such a protocol, the integrity of the data previously stored in cloud can still be verified even if the client's current secret key for cloud storage auditing is exposed. We intent to propose time period key not to be based on operations instead strongly recommend generating time period key based on logging. Time period key should be generated with long time to avoid time consumption of frequent changing of keys. The key generated should be generated automatically based on some time specification.

5. REFERANCE

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

[2] G. Ateniese, R.D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. 4th International Conference on Security and Privacy in Communication Networks, 2008

[3] F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1-6, 2008.[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MRPPDP: Multiple-Replica Provable Data Possession," Proc. 28th IEEE International Conference on Distributed Computing Systems, pp. 411-420, 2008.

[5] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Advances in Cryptology-Asiacrypt'08, pp. 90-107, 2008.

[6] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[7] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conference on Computer and Communications Security, pp. 756-758, 2010.

[8] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

[9] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.

[10] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, Vol. 62, No. 2, pp. 362-375, 2013.