EFFICIENT DATA SHARING IN CLOUD WITH THIRD PARTY AUDITOR

G Sarvanan[1], Dr. K Krishnamoorthy[2]

[1]Research Scholar, Dept of Computer Science & Engineering, Sai Nath University, Ranchi
[2] Professor, Sudarshan Engineering College, Tamilnadu

ABSTRACT

In this paper we discuss the evolvement of cloud computing paradigm and present a framework for secure cloud computing through third party auditing. The contribution of the paper is to understand the implication of cloud computing and what is meant secure cloud computing via third party auditing rather than propose a new methodology and new technology to secure cloud computing. Our holistic approach has strategic value to those who are using or consider using cloud computing because it addresses concerns such as security, privacy and regulations and compliance. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. Including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Keywords *Third party auditor, Cloud Computing, Cloud Security, Cloud service provider.*

INTRODUCTION

Cloud computing is a collection of net-centric, service oriented concepts, methodologies, best practices and technologies. It promises scaled economic benefits by provisioning computing resources and applications as services to customers while customers base their needs to subscribe related services. The services canbe computing infrastructure, storage, development and deployment platform, software services, desktop services, etc. Various issues related to Cloud computing includes Security of data from theft, Data Integrity on Cloud, Secure transmission of data to and from Cloud sever, Verifying files without much overhead/Computation , rights management, maintain security during sharing and many more. Data storage correctness or some time more generally referred as data integrity verification is one of chief Cloud security problems. Data can be altered by unauthorized entity without intimating to data owner. How would the data owner make sure that his data has not been modified by other intruders (or may be by the Cloud provider itself, accidently or intentionally). So detecting such kind of unlawful activities on data is an utmost priority issue. Data storage correctness schemes can be classified with TTP, based on who makes the verification. In case of TTP, an extra Third Party Auditor (TPA), some time in form of extra hardware or cryptographic coprocessor is used. This hardware scheme provides better performance due to dedicated hardware for the auditing process but has some drawbacks such as single TTP state across the distributed servers.

LITERATURE SURVEY

Different factors such as integrity of data, data dynamics and data privacy affects The performance of a number of approaches in cloud data storage. Each and every approach has merits and demerits which make them suitable for different applications. In this chapter we will discuss different approaches which are already carried out for cloud data security. Various mechanisms are proposed on how to use the TPA so that it can relieve the burden of data owner for local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both individuals and enterprises with high service-level requirements. This kind of audit service not only helps save data owners computation resources but also provides a transparent yet cost- effective method for data owners to gain trust in the cloud. The presence of TPA eliminates the involvement of the client by auditing whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. Though this method states how to save the computational resource and cost of storage of owner’s data but how to trust on TPA that is not calculated. If TPA modifies data or deletes some data and if it becomes intrusive and pass information of data owner to unauthorized user than how owner know about this problem is not solved. Thus, new approaches are required to solve the above problem.

WHY THIRD PARTY AUDITOR

Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform [6]. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner.

TPABASE SECURITY SCHEME

Proposed Cloud Model

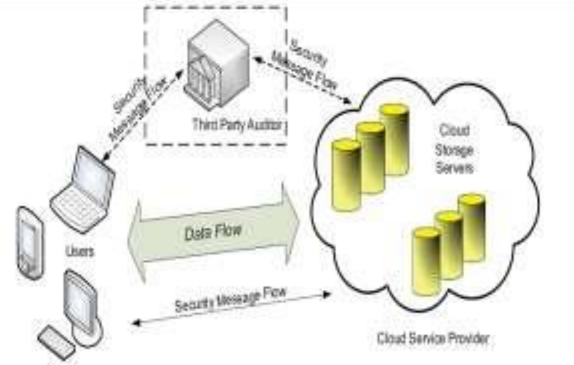

Fig. 1: Cloud data storage architecture using third party auditor (TPA)

In the figure below we prepared a model in which Client, CSP and TPA are shown. The client asks the CSP to provide service where CSP authenticate the client and provide a virtual machine by means of Software as a service. In this Vitual Machine (VM), RSA algorithm are used where client encrypt and de-crypt the file. In this VM, SHA-512 algorithms also there which make the message digest and check the integrity of data. assurance of their stored data even without the existence of local copies. In case that users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead. Note that we don’t address the issue of data privacy in this paper, as in Cloud Computing, data privacy is orthogonal to the problem we study here.

User Level Cryptography

After performing file operation it'll send the information to CSP and TPA. This CSP and TPA can keep our information not solely safe but additionally offer integrity but how it does not make sure that we are going to full trust on TPA. He will send data’s of information owner to unauthorized user. If we remove the TPA even it will not solve the matter as a result of CSP may also send the information to unauthorized user and also data owner doesn't get a bonus of TPA. Therefore cryptography is needed at user level. In this scheme encoding and decipherment is completed with the assistance of RSA formula [7]. colluding together to hide a data loss or corruption incident.

Mechanism for Data Check Integrity

As data owners no longer physically possess the storage of their data, cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading the file for its integrity verification is not a practical solution due to the high cost of input/output (I/O) and transmission cost across the network. Also it is not easy to check the data thoroughly and compare with our data. Even the loss of data and recovery of data is also not easy. Considering the large size of the outsourced data and the owner’s con-strained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for data owners. Hence, to fully ensure data security and save data owners’ computation resources, we propose to enable publicly auditable cloud storage services, where data owners can resort to an external third party auditor (TPA) to verify the outsourced data when needed.

CONCLUSION

Cloud computing security issues have brought us with great opportunities and challenges. Security in cloud computing can be addressed with TPA and without TPA. In the cloud computing by using the TPA mechanism we can increase the data security which is essentially a distributed storage system. To ensure each data access in control and reduce the complexity of cloud computing by help of Advance Encryption Technique (AES). Cryptographic techniques are used to provide secure communication between the client and the cloud. The system ensures that the client’s data is stored only on trusted storage servers and it cannot be transferred by malicious system administrators to some corrupt node. Symmetric key sharing is handled with public key cryptography, to achieve faster performance and low computational overhead. The system achieves confidentiality and integrity of the client’s data stored in the cloud. Also secure and efficient data dynamic operations such as update delete and append on the data blocks stored in the cloud. Our future goal is to design a secure cloud storage system with TPA which addresses the issues mentioned.

REFERENCES

[1] Cong Wang and KuiRen, Wenjing Lou, Jin Li, Toward Publicly Auditable Secure Cloud Data Storage Services in IEEE Network July/August 2010 [2] N. Gohring, "Amazon's S3 down for several hours," Online at http://www.pcworld.com/businesscenter/article/ 42549/amazons s3 down for several hours.html, 2008.

[3] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," *Proc. of CCS '07*, pp. 584–597, 2007.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," *Proc. of Asiacrypt '08*, Dec. 2008. [5] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175, 2008, http://eprint.iacr.org/.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," *Proc. Of CCS '07*, pp. 598–609, 2007.

[7] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," *Proc. of SecureComm '08*, pp. 1– 10, 2008.

[8] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," *Proc. of ICDCS '06*, pp. 12–12, 2006.

[9] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," *Proc. of the 2003 USENIX Annual Technical Conference (General Track)*, pp. 29–41, 2003.

[10] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report 2008/489, 2008, http://eprint.iacr.org/.

[11] L. Carter and M. Wegman, "Universal Hash Functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[12] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasurecoded Data," *Proc. 26th ACM Symposium on Principles of Distributed Computing*, pp. 139–146, 2007.

[13] J. S. Plank and Y. Ding, "Note: Correction to the 1997 Tutorial on Reed-Solomon Coding," University of Tennessee, Tech. Rep. CS-03- 504, 2003.

[14] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," *Proc. of IEEE INFOCOM*, 2009.

[15] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," *Proc. of ICDCS '08*, pp. 411–420, 2008.

[16] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and

Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.