ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Incorporation of Third Party Auditor for Safe and Secure Data Storage in Cloud Computing

Sanjeeva Polepaka
Associate Professor,
Department of CSE,
Malla Reddy Engineering College.

Mr. Rajeshwarrao kodipaka
Assistant Professor,
Department of CSE,
Malla Reddy Engineering College.

Abstract:

Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities.

Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

Introduction of domain:

Cloud Computing is one of the best choice for Small and Medium Sized Entrepreneurs' in the world. This has been used widely to cater the needs of organizations with different software applications through SAAS operations of cloud. Cloud has gifted the organizations the platform as a service at most economical rates. The economical rates and swift services has given rise to the cloud computing fame.

But the recent privacy issues and security challenges have degraded the cloud computing marketing. North Bridge (2013)1. Cloud market has fallen down because of the data storage security problems, quality of services and privacy preserving issues in cloud computing. The research scholars have done enough research to admeasure the problems but still lot of loop holes and missing links are notified in cloud computing to arrest the problems. There is a great need to revive the situation by doing the research work to ensure data storage security in cloud computing. There are many research works tried to ensure the data security in cloud computing servers with different techniques like digital encryption, fuzzy key word search etc. The ultimate solution for data security and data storages should be given to arrest the problems due to Byzantine failure, malicious data modification attack and server colluding attacks. Ricardo Puttini (2013)

Aim:

The aim of the project is to utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security. The aim is to support efficient handling of multiple auditing tasks in cloud computing. The aim is to explore the technique of bilinear aggregate signature to extend the main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. The aim includes to provide an extensive secured and highly performing system in cloud computing with an effective third party auditor.

Objectives:

•The main objective of the project is to develop a highly secured and good performance system with third party auditor for data storage in cloud computing.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

•The objective is to design and develop a cloud computing application with extensive public data storage with third party auditing system.
•The objective is to demonstrate the third party auditing system is not effecting the performance of the cloud servers and storage operations.
•The implementation of third party auditing with high performance for the public storage in cloud computing is one of the objective.
•The objective is to develop a cloud computing application with high security in storing public data.

Background:

Cloud computing is one of the most popular technological aspects in computational world. The most important thing in cloud computing is data storage with proper security measures. At the same time cloud computing is facing the data leakage and insecurity. To avoid these challenges in cloud computing a strong secured auditing system is needed to identify the users and their data. The increased security has to be implemented, at the same time the performance should not be degraded. To give proper solution the present project has been developed to provide the higher data security and increased performance while implementing the public data auditing in the cloud computing.

Existing System:

Though Cloud computing is enriched with the special features like agile, reliable, cost effective and measurable delivery of data. Cloud computing has excellent delivery models with identification, Authentication, Authorization, Confidentiality, Integrity, Non-repudiation and availability as information security requirements. it is blamed by the provision of untrustworthy servers located at remote and un-known locations. This feature has become an issue to store sensitive data and confidential data at untrusted servers at unknown remote locations and caused the heavy computation overhead. Frequently the cloud computing has encountered the security issues such as SQL Injection Attacks, Cross Site Scripting Attacks, Man in the Middle Attacks, Network Level Security Issues, DNS attacks, Sniffer Attacks, BGP Prefix Hijacking and issue of reused IP Address. Apart from these attacks Application level security issues with security concerns with the Hypervisor, Denial of Service Attacks, Cookie Poisoning, Hidden Field Manipulation. Captcha Breaking, Google Hacking and Distributed DOS Attacks are traced in cloud computing. To overcome all these attacks and computation overhead, Priyadarshini has suggested a cloud storage mechanism with Kerberos authentication and utilization of multi-clouds. Kerberos secure mechanism is very strong to protect weak link from opponent. It is very reliable with a system to back up. The Kerberos mechanism is transparent which can be revealed with the password authentication. It is measurable to support large number of clients and service providers. Kerberos authentication mechanism is rich with Authentication Servers and Ticket Granting Servers which can be incorporated in six steps. Above all these measures Priyadarshini has suggested multi-clouds environment to implement Kerberos Realms and Multiple Kerberi to obtain increased security in cloud computing storage. - A. Priyadharshini [2013].

Drawbacks of Existing system:

The Department of Education, The United States of America has incorporated a Privacy Technical Assistance Center for learning data privacy, confidentiality and security. Data security threats are classified into two types. These are technical and non-technical. A comprehensive privacy and data security plan has been initiated by PTAC to reduce the vulnerability to security threats. The technical data security threats are regarded as non-existent security architecture, Un-Patched client side Software and Application, Phishing and targeted Attacks which is known as Spear Phishing, Internet Websites, Poor configuration Management, data storage in mobile devices and transfer of data from mobile devices, Cloud Computing, Data from removable media, Botnets [the series of networks of compromised computers] and Zero-day attacks. The non technical cyber security threats are regarded as Insider attacks, Poor passwords, Physical Security, Insufficient backup and recovery, improper destruction, Social Engineering and social media. PTAC has successfully inculcate the mitigation for all above mentioned threats and suggested the students to follow consistent implementation of the security plan drastically eradicate the cyber threats and establish the security. – PTAC – IB [2011].

Proposed System:

The proposed system is developed with the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

To support efficienthandling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where Third Party Auditing can perform multiple auditing tasks simultaneously.

Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for Third Party Auditing upon delegations from multi-users.

Third Party Auditing:

Third party auditing system is one security mechanism to store the data into the cloud servers. Third party auditing system is arranged by the cloud consumers as well as the cloud service providers. The cloud service providers would safe guard the server with the help of Third party auditing.

Third party auditing will scan the data whatever stored by the cloud consumer then it will decide whether the data can be stored in the server or not. If the data consists of malicious data then the TPA will delete the data from the server. Predominantly the data storage will be audited by the TPA system and allow the data to place in the server. It can be accessed by the authorized user of the Cloud Consumers.

Algorithm:

A public auditing scheme consists of four algorithms. These are KeyGen, SigGen, GenProofand VerifyProof.

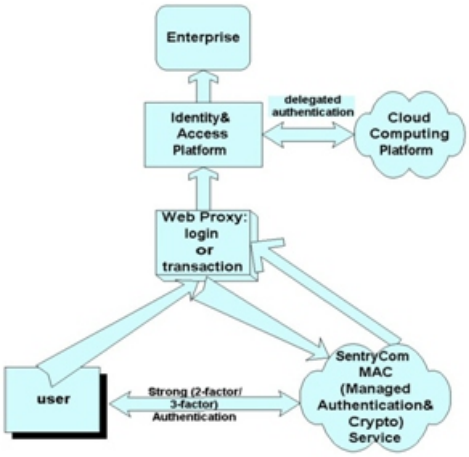
•KeyGen: key generation algorithm that is run by the user to setup the scheme

•SigGen: used by the user to generate verification metadata, which may consist of MAC, signatures or other information used for auditing

•GenProof: run by the cloud server to generate a proof of data storage correctness

•VerifyProof: run by the TPA to audit the proof from the cloud server.

Flowchart:



Modules:

1.Privacy-Preserving Public Auditing Module:

Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator.

Overview to achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF).

The proposed scheme is as follows:

•Setup Phase

•Audit Phase

2.Batch Auditing Module:

With the establishment of privacy-preserving public auditing in Cloud Computing, TPA may concurrently handle multiple auditing delegations upon different users' requests. The individual auditing of these tasks for TPA can be tedious and very inefficient. Batch auditing not only allows TPA to perform the multiple auditing tasks simultaneously, but also greatly reduces the computation cost on the TPA side.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

3.Data DynamicsModule:

Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. We can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics.

The Functionality of the Project:

The project is designed and developed to demonstrate the cloud computing data storage security with the help of Third Party Auditing system. The cloud computing is declining with the security loopholes. These loop holes of security system can be arrested by employing the third party auditing system. The cloud computer is occupied by the cloud consumers. Sometimes the cloud servers are losing the data integrity and confidentiality because of the cloud consumer's data stealing mechanism. The data stored by the cloud consumers should be streamlined by employing a third party auditor who is most amicable and trustworthy for cloud consumers as well as cloud service providers. The cloud consumer's data should be scanned and verified by the Third Party Auditor, then it should be stored in the cloud servers. This data streamlining mechanism will avoid the malicious data storage in the cloud computing servers. When the data is accessed by the cloud users who are created and permitted by the consumers should also approved by the third party auditor. In this present project the Third Party Auditing system will keep an eye on the data accessing items and keeps the track of them. In this way the data storage mechanism will be audited by the Third Party auditor and safely enable the cloud consumer to store the data into the cloud servers.

Conclusion :

The project is designed with a novel mechanism to audit the data storage with third party auditing system to filter the data. The data storage options have to be streamlined with proper monitoring and auditing system. To ensure the safe and secure data storage mechanism in cloud computing the proposed third party auditing system is developed in .Net technologies in simulation mode. This has been tested with proper test cases to ensure the mechanism working properly. The test results have been evaluated.

Public auditability also allows clients to delegate the integrity verification tasks to TPA while they themselves can be unreliable or not be able to commit necessary computation resources performing continuous verifications. Another major concern is how to construct verification protocols that can accommodate dynamic data files. In this paper, we explored the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in Cloud Computing.

References:

1.P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009.

2.M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

3.N. Gohring, "Amazon's s3 down for several hours," Online at http://www.pcworld.com/ businesscenter/article/142549/amazons s3 down for several hours.html, 2008.

4.Amazon.com, "Amazon s3 availability event: July 20, 2008," Online at http://status.aws.amazon. com/s3-20080720.html, July 2008.

5.S. Wilson, "Appengine outage," Online at http://www.cio-weblog.com/50226711/appengine outage. php, June 2008.

6.B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at http://voices.washingtonpost. com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.

7.G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," Cryptology ePrintArchive, Report 2007/202, 2007, http://eprint. iacr.org/.

8.M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

9.Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, Saint Malo, France, Sep. 2009.

10.Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www.cloudsecurityalliance.org.

11.H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

12.Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.

13.M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

14.104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996, last access: July 16, 2009.

15.D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signaturesfrom bilinear maps," in Proc. of Eurocrypt 2003, volume 2656 of LNCS. Springer-Verlag, 2003, pp. 416–432.

16.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.

17.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.

18.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/.

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

20.J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed ErasurecodedData," Proc. 26th ACM Symposium on Principles of Distributed Computing, pp. 139–146, 2007.

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

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

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

24.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/.

25.M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop on Hot Topics in Operating Systems (HOTOS '07), pp. 1–6, 2007.