International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Privacy Conservation and Public Inspection for Secure Cloud Storage

Sahar Jasim Hussein[1], Hemant Mahajan[2]

[1]Modern Collage of Arts, Science and commerce, Pune

[2]Director and Research Analysis, Godwit Technologies Pvt. Ltd.

Abstract: ***Using Cloud Storage, users will remotely store their information and revel in the on-demand top quality applications and services from a shared pool of configurable computing resources, while not the burden of native information storage and maintenance. However, the very fact that users now not have physical possession of the outsourced information makes the info integrity protection in Cloud Computing a formidable task, particularly for users with affected computing resources. Moreover, users ought to be able to simply use the cloud storage as if it's native, without concern concerning the requirement to verify its integrity. therefore, sanctioning public audit ability for cloud storage is of important importance so users will resort to a 3rd party auditor (TPA) to ascertain the integrity outsourced information and be worry-free. Now a day's secure information storage over cloud servers is a very important analysis issue within the field of cloud computing, albeit numerous ancient approaches are there for cloud storage, however they're not best, as a result of several of the standard mechanisms aren't best for information correctness, integrity and dynamic information support. during this paper we tend to are introducing associate economical mechanism for information correctness and error detection, for the implementation purpose we tend to simulated the system with the new design.***

Keywords: Data storage, privacy preserving, public auditability, cloud computing, delegation, batch verification, zero knowledge.

1. Introduction

Cloud Computing has been visualised because the next generation design enterprise of IT as a result of its long list of unprecedented blessings within the IT history: on-demand world organization ambiguities and self-service, network access location freelance pooling of resource, additional resource physical property, usage-based valuation and transference of risk .As a riotous technology with profound suggestion, over Cloud Computing is reworking the terribly nature of however businesses use IT and One basic facet of this paradigm shifting is that information is being centralized or outsourced cloud and From users perspective, as well as each people and enterprises of IT, information storage remotely into the cloud in a very versatile on-demand manner brings appealing benefits: relief of the burden for management of storage and universal information access with freelance abstraction locations and dodging of cost on hardware, software, and personnel maintenances, other. Whereas Cloud Computing makes these blessings additional appealing, however ever it conjointly brings new and difficult security threats towards users' outsourced information. Since cloud service suppliers (CSP) square measure separate body objects, outsourcing of knowledge is really relinquishing user's final management over the fate of their data.

A growing variety of on-line services, like Amazon, Yahoo!, Google, Snappish, and Mazy.com,aim to profit by storing and maintaining countless valuable user information. Example uses of this storage embrace on-line backup, email, pic sharing, and video hosting. Several of those services provide little quantity of ―teaser" storage for free of charge, and charge for larger, upgraded versions of the service.

Studies of deployed large-scale storage systems show that no storage service is utterly reliable; all have the potential to lose or corrupt client information. Today, a client that wishes to consider these services should build associate degree uneducated selection. He has solely negative interesting anecdotes on that to base his call and repair quality or ―brand name" isn't a positive indicator of dependableness [10]. to understand if his information is safe, he should either blindly trust the service or laboriously retrieve the hosted information whenever he needs to verify its integrity, neither of that is satisfactory. Sadly, to date, there aren't any truthful and specific mechanisms for creating these services in control of information loss.

Cloud computing gave a path to information outsourcing. information outsourcing to cloud storage servers is raising trend among several companies and users attributable to its financial blessings. this can be in essence means the consumer nothing however owner of the information moves its data to a 3rd party cloud storage server that genuinely stocks up the information with it and provide it back to the consumer whenever needed. associate degree enterprise deals with voluminous quantity of knowledge. Generation of knowledge is incredibly straightforward however the storage of knowledge wants the hardware to be updated oftentimes so as to convey house to the massive volume of knowledge. additionally, to information storage information maintenance conjointly poses large downside.

Storage outsourcing of knowledge to cloud storage helps such companies by reducing the prices of storage, maintenance and personnel. It may also assure square measure liable storage of vital information by keeping multiple copies of the knowledge thereby reducing the possibility of losing data by hardware failures.

Cloud computing provides answer to each these issues in an efficient manner. It's a pay per-use model during which the supplier is customised by suggests that of a group of Service Level Agreements (SLAs). SLA offers guarantees to the supplier and consumer Organizations and people will enjoy

mass computing and storage centres, provided by giant corporations with stable and powerful cloud architectures. Storing of user information within the cloud has its own blessings and ends up in several attention-grabbing security queries which require to be inspected extensively for creating it a reliable answer to the matter of avoiding native storage of knowledge. several issues like information authentication and integrity arises once outsourcing the information. to make sure information security the cloud supplier stores the information in associate degree encrypted type.

2. Literature Survey

T. Schwarz and E.L. Miller, [31]. The rising use of the web for remote storage and backup has LED to the matter of substantiate that storage sites in a very distributed system so store info this should typically be exhausted the absence of data of what the data ought to be. we have a tendency to use Mn erasure-correcting secret writing to safe-guard the keep knowledge and use algebraically signatures—hash functions with algebraically properties—for verification. Our theme primarily utilizes one such algebraically property: taking a signature of parity provides identical result as taking the parity of the signatures. to create our theme collusion resistant, we have a tendency to blind knowledge and parity by XORing them with a pseudo-random stream. Our theme has 3 benefits over existing techniques.

F. Sebe, J. Domingo-Ferrer, A. Martı´nez-Balleste, Y. Deswarte, and J.-J. Quisquater, the event of knowledge data society has caused a huge majority of such infrastructures to vitally depend upon the right operation of the underlying info systems—that is why such info systems are typically stated as a critical information infrastructure. Indeed, any service interruption, malfunction or, even worse, partial or total destruction of these info systems as an on sequence of associate accident or a coup de main may end up in Brobdingnag Ian material or maybe human casualties. This reality supports the claim that one amongst the largest challenges in infrastructure protection is that the underlying info security problem: info systems ought to be dependable.

G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kisser, Z. Peterson, and D. Song, [9], The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, that drastically reduces I/O prices. The consumer maintains a relentless quantity of information to verify the proof. The challenge/response protocol transmits a little, constant quantity of information, hitch minimizes network communication. Thus, the PDP model for remote knowledge checking supports giant knowledge sets in widely-distributed storage systems. We gift 2 provably-secure PDP schemes that square measure additional economical than previous solutions, even compared with schemes that come through weaker guarantees. Specially, the overhead at the server is low (or even constant), as critical near within the size of the info. Haritha Nuthi Hemalatha Goli,

Ramakrishna Mathe, [13], exploitation cloud storage users may be able to store their knowledge while not bothering regarding its storage correctness. So, the user won't have any confirmation regarding the outsourced knowledge. The cloud knowledge storage ought to have some mechanism to verify storage correctness and its integrity. All the prevailing technique will verify the integrity of outsourced knowledge on condition that the info is static. during this paper we have a tendency to propose a privacy protective public auditing for secure cloud storage that supports dynamic knowledge and batch auditing. C. Wang, Q. Wang, K. Ren, and W. Lou, [22], By exploitation Cloud storage, users will access applications services, computer code whenever they need over the web. Users will place their knowledge remotely to cloud storage and acquire advantage of on demand services and application from the resources. The cloud should need to guarantee knowledge integrity and security of information of user. the problem regarding cloud storage is integrity and privacy of information of user will arise. to take care of two overkill this issue here, we have a tendency to square measure giving public auditing method for Cloud storage that users will build use of a third-party auditor(TPA) to envision the integrity of information. Not solely verification of information integrity, the projected system additionally supports knowledge dynamics. The work that has been wiped out this line lacks knowledge dynamics and true public auditability. The auditing task monitors knowledge modifications, insertions and deletions. The projected system is capable of supporting public audit ability, knowledge dynamics and Multiple TPA square measure used for the auditing method. we have a tendency to additionally extend our thought to ring signatures within which HARS theme is employed. Merkle Hash Tree is employed to improve block level authentication. additional we have a tendency to extend our result to alter the TPA to perform audits for multiple users at the same time through Batch auditing.

3. Mathematical Model

Step 1: Input Data: file, User name, Pass
Output Data: Secured File
1. Generate the random set

$$\{(i, \nu_i)\}_{i \in I};$$

$$\xrightarrow[\text{challenge request chal}]{\{(i,\nu_i)\}_{i \in I}}$$

Step 2: Compute

$$\mu = \sum_i \nu_i m_i;$$

Step 3: Compute

$$\sigma = \prod_i \sigma_i^{\nu_i};$$

Step 4: Compute R using

$$\{H(m_i), \Omega_i\}_{i \in I};$$

Step 5: Verify

$$sig_{sk}(H(R))$$

Step 6: Verify

$$\{m_i\}_{i \in I}.$$

4. Work Done

In this section we are discussing the practical environment, scenarios, performance metrics used etc.

4.1 Input

In this Training and Testing Image is the input for our practical experiment.

4.2 Hardware Requirements

Processor: Pentium IV 2.6 Ghz
Ram: 512 Mb
Hard Disk: 20 Gb

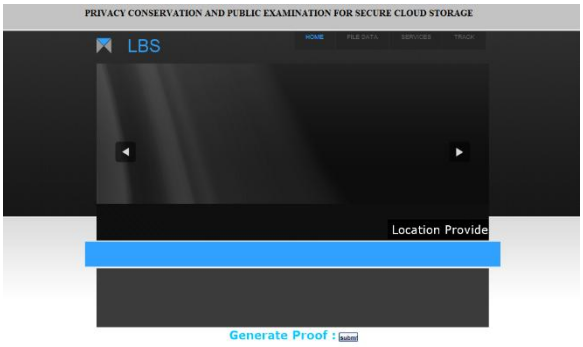
4.3 Software Requirements

Front End: J2SE
Back End: MySQL 5.1
Tools Used: Net Beans 7.2.1 or above
Operating System: Windows 7/8

4.4 Results of Practical Work

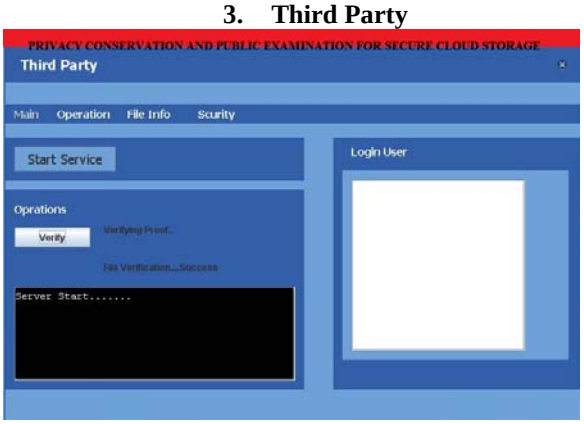
Following figures are showing results for practical work which is done. Following figure showing the main screen. That takes the input data set,

1. Cloud Server

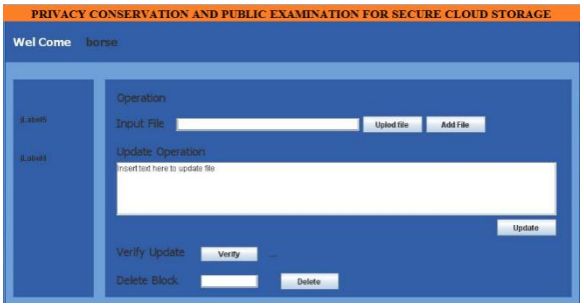


2. Admin Login

3. Third Party



4. User GUI



5. Conclusion and Future Work

In this paper, we tend to propose a privacy-preserving public auditing system for information storage security in cloud computing. we tend to utilize the homomorphic linear appraiser and random masking to ensure that the TPA wouldn't learn any data concerning the info content hold on the cloud server throughout the economical auditing method, that not solely eliminates the burden of cloud user from the tedious and presumably costly auditing task, however additionally alleviates the users' concern of their outsourced information leak. Considering TPA might at the same time handle multiple audit sessions from completely different users for his or her outsourced information files, we tend to more extend our privacy-preserving public auditing protocol into a multiuser setting, wherever the TPA will perform multiple auditing tasks in a very batch manner for higher potency. we tend to area unit given the privacy –preserving public auditing theme that supports information dynamic operations. Public auditing theme supports hashing technique. the info dynamic operations will get performed by victimisation Merkle Hash Tree(MHT). we tend to use multiple TPA for the auditing method that handles multiple users through batch auditing.

References

[1] C. Wang, Q. Wang, K. Ren, a n d W. Lou, ―Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM "10, Mar.2010.
[2] P Mell and T. Grance, ―Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloud-computing /index.html, June 2009.

[3] Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing,3-42.
[4] Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010
[5] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail disaster reports-of-mass-email deletions/,2006.
[6] J. Kincaid, "Miramax/The Linkup Closes Its Doors," http://www.techcrunch.com/2008/07/10/mediamaxtheli nkup-closesits-doors, July 2008.
[7] Amazon.com, "Amazon S3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.
[8] S. Wilson, "Appengine Outage," http://www.cio-weblog.com/ 50226711/appengine_outage.php, June 2008.
[9] B. Krebs, "Payment Processor Breach May Be Largest Ever," http://voices.washingtonpost.com/securityfix/2009/01/ payment_processor_breach_may_b.html, Jan. 2009.
[10] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Irretrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
[11] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Irretrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
[12] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance.org, 2009.
[13] H. Shacham and B. Waters, "Compact Proofs of Irretrievability," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asia crypt), vol. 5350, pp. 90-107, Dec. 2008.
[14] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[15] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (Hoot's '07), pp. 1-6, 2007.
[16] 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.
[17] R. Curtmola, O. Khan, and R. Burns, "Robust Remote Data Checking,"Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (Storages '08), pp. 63-68, 2008.
[18] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Irretrievability: Theory and Implementation,"Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 43-54, 2009.
[19] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," J.Cryptology, vol. 17, no. 4, pp. 297-319, 2004.
[20] A.L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical Short Signature Batch Verification," Proc. Cryptographers' Track at the RSA Conf. 2009 on Topics in Cryptology (CT-RSA), pp. 309-324, 2009.
[21] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data possession," Proc. Int'lConf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10, 2008.
[22] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans.Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012.
[23] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.
[24] R.C. Merkle, "Protocols for Public Key Cryptosystems,"Proc. IEEE Symp. Security and Privacy,1980.
[25] G. Ateniese, S. Kamara, and J. Katz, "Proofs of Storage from Homomorphic Identification protocols,"Proc. 15th Int'l Conf.Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT), pp. 319-333, 2009.