International Journal of Advanced Technology and Innovative Research

www.ijatir.org

ISSN 2348–2370
Vol.06,Issue.11,
November-2014,
Pages:1375-1378

Third Part Auditor (TPA) & Multi-Authority System (MAS) using Cloud Service Provider Agent (CSPA) to Provide Privacy Preserving Cloud Storage

INGALLIGI SATYA RAJ
Research Scholar, Dept of CSE, S S Institute of Technology, India, E-mail: satya.raj810@gmail.com.

Abstract: Cloud storage can be utilizable for users to store their data remotely and access the on-demand applications and accommodations from shared pool of configurable computational resources, therefore no desideratum of local data storage and maintenance. However there is situation in this that the utilizer does not have the physical possession of the outsourced data therefore the data integrity aegis and data consistency auspice is very paramount task, especially for the users who possess constrained number of computing resources. Moreover the cloud users must be able to utilize the cloud storage just like the local storage, without worrying about to the desideratum to verify the data integrity and data consistency. To achieve this public auditability for cloud storage can be utilizable. Users can rely on the third party auditor (TPA) on the behalf of cloud utilizer so that the cloud utilizer is worry free. By introducing TPA the care should be taken so that incipient susceptibilities towards data privacy should not be integrated and withal no adscititious online communication burden to cloud utilizer. Cloud computing environments impose incipient challenges on access control techniques due to the growing scale and dynamicity of hosts within the cloud infrastructure; we proposed Multi-Ascendancy System (MAS) architecture. This architecture consists of agents: Cloud Accommodation Provider Agent (CSPA), Control Agent (CA), Third party Auditor (TPA) and Attribute Ascendancy Agent (AAA). The TPA provides a graphical interface to the cloud utilizer that facilitates the access to the accommodations offered by the Cloud Accommodation Provider (CSPA). In this paper we proposed a privacy preserving third party auditing for securing users data on cloud storage. We further enhance our system to enable the TPA to perform multiple auditing tasks simultaneously and efficaciously.

Keywords: Third Part Auditor (TPA), Data Privacy, Cloud Computing, Multi-Authority System(MAS), Cloud Service Provider Agent(CSPA), Privacy Preserving, Cloud Storage.

I. INTRODUCTION

Cloud computing has been critical consequentiality in the incipient era of information technology. It enables the users to store their data on the remote cloud storage space which is available on the cloud server. By storing data on the cloud server utilizer has no desideratum to maintain the local facsimile of such data thus preserving the resources of utilizer withal utilizer is in liberty to access its data anytime anywhere on-demand. When data stored on the cloud storage it is critical paramountcy for cloud accommodation provider (CSP) to provide utilizer the environment like the users data stored on the local storage. Though user's data stored on the cloud storage it must appear as it is local to utilizer. Utilizer must capable of doing all the operations on the data which can be performed on it when it is local without affecting the users experience for accessing, updating and retrieving the data. To ascertain utilizer for integrity, consistency and privacy of user's remote data there must be some provision to verify data integrity, data consistency and correctness. The traditional approach to achieve this is to retrieve consummate data from cloud storage to the local storage and verify it. This method is tedious and inefficient and it has to utilize higher communication and computational overhead on network.

Cloud storage is composed of thousands of storage contrivances clustered by network, distributed file systems and other storage middleware to provide cloud storage accommodation for cloud users. The typical structure of cloud storage includes storage resource pool, distributed file system, accommodation level acquiescents (SLAs), and accommodation interfaces, etc. Ecumenically, they can be divided by physical and logical functions boundaries and relationships to provide more compatibilities and interactions. Cloud storage is inclining to coalesced with cloud security, which will provide more robust security [1].Cloud Data access control issue is mainly cognate to security policies provided to the users while accessing the data. In a typical scenario, a diminutive business organization can utilize a cloud provided by some other provider for carrying out its business processes. This organization will have its own security policies predicated on which each employee can have access to a particular set of data.

The security policies may entitle some considerations where in some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to eschew intrusion of data by unauthorized users [2, 3, 4]. In case of dynamic data this method is of highly impractical. One solution for this is to perform auditing task by third party auditor (TPA). TPA can perform the auditing on behalf of utilizer and provide audit

report to the utilizer. This technique is additionally utilizable for cloud accommodation provider (CSP) to maintain its reputation by getting higher reliability, consistency and data integrity ratings or certificates from TPA, So as to amend their business on commercial perspective. But this approach does not consider the data privacy bulwark of the user's data on the cloud storage. TPA can leak user's data intentionally for achieving profit from selling the users private data.

II. RELATED WORK

A. Existing System

Since cloud accommodation providers (CSP) are discrete administrative entities, data outsourcing is authentically relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put in peril due to the following reasons. First of all, albeit the infrastructures under the cloud are much more puissant and reliable than personal computing contrivances, they are still facing the broad range of both internal and external threats for data integrity.

Disadvantages of Existing System: Albeit outsourcing data to the cloud is economically captivating for long-term sizably voluminous-scale storage, it does not immediately offer any assurance on data integrity and availability. This quandary, if not felicitously addressed, may impede the prosperity of cloud architecture. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purport of data security auspice cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those unaccessed data and might be too tardy to instaurate the data loss or damage.

B. Proposed System

To plenarily ascertain the data integrity and preserve the cloud users' computation resources as well as online burden, it is of critical paramountcy to enable public auditing accommodation for cloud data storage, so that users may resort to an independent third party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more more facile and affordable way for the users to ascertain their storage correctness in the cloud. Moreover, in additament to avail users to evaluate the jeopardy of their subscribed cloud data accommodations, the audit result from TPA would withal be salutary for the cloud accommodation providers to amend their cloud predicated accommodation platform, and even accommodate for independent arbitration purposes. In a word, enabling public auditing accommodations will play a consequential role for this nascent cloud economy to become plenarily established, where users will require ways to assess risk and gain confide in the cloud.

Advantages of Proposed System:

- We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user's cloud data without learning the data content.
- To the best of our cognizance, our scheme is the first to fortify scalable and efficient privacy preserving public storage auditing in Cloud. Concretely, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.
- We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

III. IMPLEMENTATION

The incipient paradigm for cloud computing. Data aegis as an accommodation is the paradigm designed in this paper. The authors additionally used two different approaches to data privacy they are plenary-disk encryption and computation on encrypted data. In the full-disk encryption (FDE) the entire physical disks are encrypted for the simplicity and speed. The plenarily homomorphic encryption (FHE) is utilized for computation on cipher texts. When comparing FDE and FHE, the FDE has high performance than FHE. The access control list is utilized for the utilizer access. The same phenomenon can be utilized in the batch process, but it has a different logging granularity. Some of the challenges in this paper are how to migrate for subsisting applications and can technology be standardized across platforms [3]. The privacy-preserving public auditing system for data storage security in cloud computing. The privacy preserving fortifies the public auditing without the retrieval access of entire data blocks.

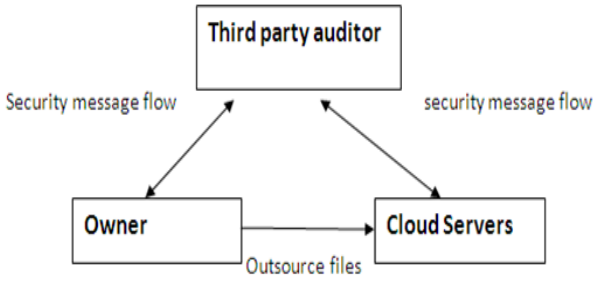

Fig.1. Automatic Protocol Blocker.

The public auditing scheme has four algorithms they are KeyGen, SigGen, GenProof, Verify Proof. The privacy preserving public auditing fortifies for batch auditing. Third Party Auditor (TPA) can handle multiple auditing delegations between different users request. But the individual auditing is very arduous in TPA. So the author

deals that we can utilize TPA to perform the multiple auditing tasks in a batch process concurrently. The auditing system in the cloud server is been illustrated in fig 1.The block of message is sent to the auditor for checking integrity [4].

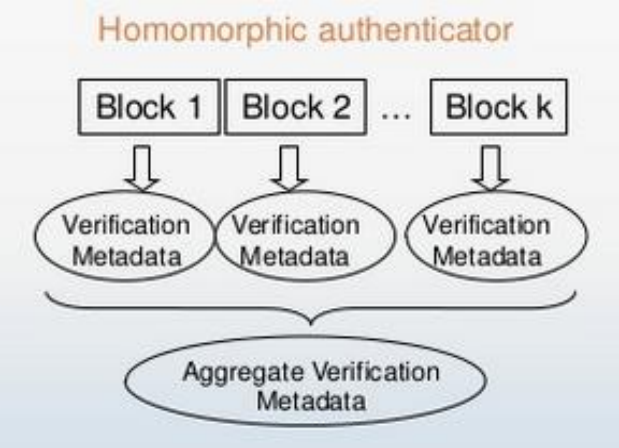

Fig.2. Homomorphic Authenticator.

To fortify efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to elongate our main result into a multi-utilizer setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient as shown in Fig.2. We withal show how to extent our main scheme to fortify batch auditing for TPA upon delegations from multi-users.

A. Third Party Auditor

In this module, Auditor views the all utilizer data and verifying data .Auditor directly views all utilizer data without key. Admin provided the sanction to Auditor. After auditing data, store to the cloud.

B. Cryptography

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

C. Cloud Computing

Cloud computing is the provision of dynamically scalable and often virtualized resources as a accommodations over the cyber world Users need not have erudition of, expertise in, or control over the technology infrastructure in the "cloud" that fortifies them. Cloud computing represents a major transmutation in how we store information and run applications. In lieu of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud"—an assemblage of computers and servers accessed via the Internet.

D. Privacy-Preserving

To ensure that the TPA cannot derive users' data content from the information Collected during the auditing process.

IV. EXPERIMENTAL RESULT

Experimental results of this paper is shown in Figs.3 to 7.

Fig.3. System Home Page.

Fig.4. User Login Page.

Fig.5. File Upload Page.

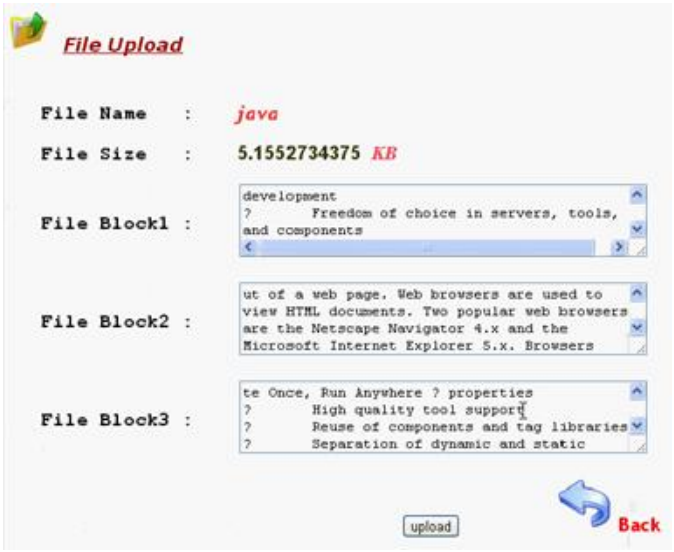

Fig.6. Uploaded File Division Page.

Fig.7. Uploaded File with Encrypted form.

V. CONCLUSION

In this system there is more fixate on auditing task for ameliorating reliability by integrating more intricacy in auditing process. We are proposing different approach in which in lieu of integrating more intricacy in auditing we fixate on integrating clustered TPAs and reducing intricacy of subsisting protocol as well as reducing the execution time. we proposed an efficacious data access control scheme for multi-ascendancy cloud storage systems, IACMACS. We additionally construct an incipient multi-ascendancy CP-ABE scheme, in which the main computation of decryption is outsourced to the server. We further designed an efficient attribute revocation method that can achieve both forward security and rearward security. Our attribute revocation methods incurs less communication cost and less computation cost of the revocation, where only those components associated with the revoked attribute in the secret keys and the ciphertext need to be updated. Through the analysis and the simulation, we showed that our IAC-MACSS is provably secure in the desultory oracle model and incurs less storage overhead, communication cost and computation cost, compared to subsisting schemes.

VI. REFERENCES

[1] G. EasonKrebs, "Payment Processor Breach May Be Largest Ever," Online at, http://voices.washington post.com/ securityfix/2009/01/paymentprocessorbreachmayb.html,Jan. 2009.

[2] 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, volume 5789 of LNCS Springer-Verlag, Sep. 2009, pp. 355–370.

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

[4] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song. Provable data possession at untrusted stores. In Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, pages 598–609,2007.

[5] P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Tech. Rep., 2009.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy (S&P'07). IEEE Computer Society, 2007, pp. 321–334.

[7] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure ealization," in Proceedings of the 4th International Conference on Practice and Theory in Public Key Cryptography (PKC'11). pringer, 2011, pp. 53–70.

[8] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP'08). Springer, 2008, pp. 579–591.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrustedstores," in Proc. Of CCS'07, Alexandria, VA, October 2007, pp. 598–609.