ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 5, Issue 2 (Apr. - Jun. 2017)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2017)

Privacy Preserved Public Auditing in Cloud Storage System

[I]Reshma B, [II]Dr.Sanjay Srivastava
[I]PG Student, Dept. of CS&E, MGM CoET, Noida, India
[II]Associate Professor, Dept. of CS&E, MGM CoET, Noida, India

Abstract
Cloud storage is gaining popularity nowadays because it allows flexible on-demand data outsourcing services with attractive benefits like relieving users from the burden of storage management, location independent universal data access facility, and reducing expenditure on user has to spend on software, hardware and personal maintenance. Having said this it is also true that this new model of data hosting service also has few security threats towards data stored on cloud, thus making individuals or enterprisers still feel reluctant to use cloud storage. The very idea of data owners losing control over their data is obviously worrisome. Thus, the availability, correctness and integrity of data are being put at risk. The cloud service providers(CSP) might cheat owners by trying to hide loss or corruption of data and claim that the files are still correctly stored in the cloud for monetary and reputation reasons. Therefore there arises an obvious necessity for users to implement an efficient protocol which can perform verification of the outsourced data on a periodical basis to make sure that the cloud indeed maintains their data intact.

Keywords
Cloud Storage, Third Party Auditor, Public Auditing, Proxy.

I. Introduction

Cloud computing is the latest technology which enables convenient network access to a pool of configurable computing resources. Cloud Computing is the most awaited technology which would allow users to remotely store data in the clouds and to enjoy the on-demand high quality services and applications from a shared pool of configurable computing resources. Outsourcing their data on cloud relieves users from the burden of local data storage and its maintenance aspects. But, the fact that users would no longer have physical possession of the large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially redoubtable task, specially for those users with limited computing resources and capabilities. Therefore, enabling public audit ability for data storage on cloud is of utmost necessity for users can opt for an external audit party to check the data integrity whenever necessary. Secure introduction of a Third Party Auditor(TPA) involves the following basic requirements to be satisfied:

1) Efficient auditing of the data stored on cloud has to be done by TPA without demanding any local copy of the data. It is also necessary that TPA, in no way, introduce any additional on-line burden to the user of the data.
2) The implementation and use of Third Party Auditor should be in no way harmful to user's data privacy. In this paper, we employ and combine homomorphic authenticator which is public key based with a random masking to achieve privacy-preserving public cloud data auditing system, to meet all the above requirements. To regenerate the failed authenticators, we also introduce a proxy. Our system is privacy preserving since neither the proxy nor the TPA has access to the user's data stored on cloud. Security and performance analysis of our system proves that the proposed scheme is secure and highly efficient.

II. Motive Of The Project

Cloud Computing offers many advantages but also brings security threats to the data stored on cloud. When user stores data on cloud, he loses his control over data which make many data owners feel reluctant to store their data on cloud. Storing data on cloud is giving up the control of data to a separate administrative entity called Cloud Service Provider(CSP). Because it it not the owner but a third party who has the control over data, there arises a suspicion on the correctness of the stored data. In other words, owner's confidential data is being put at risk. The reasons for that are as follows. Users no longer own the control over fate of their data so, conventional cryptographic primitives protection can not be directly adopted for the purpose of data security. Therefore, how to efficiently verify the integrity of outsourced data without a local copy of data files turn outs to be a big challenge for data storage security in Cloud Computing. Simply downloading data for verification of its correctness is not a practical solution due to the extortionate input output cost and transmission of the file across the network. Apart from that, it is often inadequate to detect data corruption when accessing data, as this might be too late for recovering the data loss or damage. Taking into consideration, the large size of the outsourced data and limited resource capability of the user , ability to audit the integrity of the data in a cloud environment can be frightening and extortionate for the cloud users. Thus, to completely ensure data security and to save data owner's computation resources, it is of high importance to enable public audit ability for cloud data storage so that the users may opt to a third party auditor (TPA), who has more expertise and capability that the cloud users, to audit the outsourced data whenever necessary. Based on the audit result, Third party auditor would release an audit report, which would help users to assess the risk of their subscribed cloud data service and also would be beneficial for the cloud service provider to improve their cloud based service platform. To sum up, usage of public risk auditing protocols will contribute majorly for this budding cloud economy to become fully established, where users will need ways to assess risk and gain trust in Cloud storage technology. Incase the Third party auditor fails, a proxy is also established to regenerate the authenticator.

III. Existing System

Many researches have taken place in the past regarding introducing various mechanisms to deal with the correctness of the outsourced data without demanding a local copy under different system and security models. The most important research among these works are the Proof Of Retrievability(POR) model and Provable Data Possession(PDP) model which were initially proposed for single-server scenario by Juels, Ateniese et al. and Kaliski, respectively.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Considering that files are striped and stored across multi-servers or multi-clouds redundantly, explored were the integrity verification schemes suitable for such multi-servers or multi-clouds settings with different redundancy schemes, such as erasure codes, replication and more recently, regenerating codes.

Disadvantages

a. Users may want to go through the complexity in verifying and reparation.
b. The overhead of using cloud storage is maximum since users are expected to perform too many operations to the outsourced data.
c. The auditing schemes demanded the users to always stay online, which inhibit its adoption in practice, especially for long-term archival storage.
d. The single point failure of Third Party Auditor is a major threat to the public auditing system.

IV. Proposed System

Considering that the cloud user usually possesses limited computation and memory capacity, it is important for us to reduce his overhead. Secondly, unlike traditional erasure code based cloud storage, a fixed file layout does not exist in the regenerating code based cloud storage. During the repair phase, it computes out new blocks, which might be entirely different from the faulty ones, with high probability.

Over the systems which demanded the cloud user to carry out the auditing process, we introduce public auditing methodology. We establish an entity to carry out auditing on behalf of user called Third Party Auditor. We implement a semi trusted proxy between the user and cloud. The proxy gets authentication from the user and collects the data which needs to be signed and then uploads to cloud. The public verifier or TPA cannot get any knowledge about user's data. This method is at risk when the proxy server itself gets failed.

Advantages:

a. Our System introduces public auditing system for regenerating code- based cloud storage.
b. A Third Party Auditor is implemented to perform the auditing process.
c. Since TPA is given the delegation of public auditing, users are relieved from the burden of auditing the data stored on cloud.
d. If incase the authenticator fails, a proxy is introduced to regenerate the authenticator.
e. Thus, our system strives to completely release online burden for users, making cloud storage utilization a stress free work.
f. By making use of the linear subspace of the regenerating codes, the authenticators can be computed efficiently.
g. Our scheme completely releases the cloud users from online burden for regeneration of blocks and authenticators at faulty servers and it also provides the repairing privilege to a proxy.
h. Entire system is Provable secure under random oracle model against adversaries.

V. Requirements Specification

A. Objective

Requirement Specification is used for the correct and clear function description for developing system. Developer considers Requirement Specification as reference while developing software. The Requirement Specification also gives guarantee for a customer to gain some information about issues to be solved. It divides the issues into component parts. While specifying the design, the Requirement Specification is taken as input.

The specification for requirement gives a full explanation about the system performance. Requirement Specification also specifies non functional needs. This would aid in helping as suggestions during the process of designing the software. The Requirement Specification is called as parent document since it contains all the necessary documents for managing the project such as design requirements, working flow, architecture and testing plan.

B. Functional Requirements

Functional requirement is to specify the function of software and components. The input, process and output are given by the function. It also gives the data which can be changed according to the system behavior along with testing the various possibilities of functions for software system. In other words, it describes the behavior of system. An example of process of input, processing and output is as follows

- Upload the files block wise to cloud
- User sends authentication rights to auditor
- Auditor manages the files
- Proxy generates damage files
- Auditor verifies files and sends to the user

C. Non-Functional Requirements

Cost: The expenditure incurred in the development of the system is the aggregated value of that spent on required hardware, software resources and also the man power. All these factors contribute to the total cost incurred in the development of the system. Strive to make the cost minimum for it to be deployed with a light budget.

Quality: Regeneration can possibly improve the efficiency of data storage and access to owner with the correct or original owner's data in cloud computing by reducing the access latency and bandwidth usage.

Performance: The data which are outsourced to cloud should be safe as possible and performance provided by the service provider should be high.

Usability: The space available on cloud should be utilized efficiently by the cloud users.

Availability: The cloud resource is available 24x7.

Safety: The system will notify the respective data owner when a data quality or data loss issue arises.

Security: Only data owner is permitted to access and make modifications to the data stored on cloud. It is kept safe from unauthorized access.

Scalability: Based upon the demand, cloud usage can be scaled up or down.

D. System Requirements

Hardware Requirements: A Pentium-III processor with 1.1GHz speed and 256MB RAM is the minimum requirement along with Hard disk size of 20GB and floppy drive 1.44MB for the design of the proposed system.

Software Requirements: A system with Windows XP/7, Tomcat

5.0 server, Mysql 5.0, JDBC is the minimum requirement. Java script and JSP is used for the design of the proposed system.

IV. Conclusion

In the proposed paper, the various security threats regarding cloud data storage has been brought into limelight. Various techniques and methods which facilitate privacy preserving public auditing system for secured data storage have been studied. A Third party auditor is established for data integrity checking on behalf of the user. The various methods for secured public auditing are discussed. The motive of the proposed paper is briefed.

The existing system along with its disadvantages is discussed. The new methodologies that we have come up with is explained in detail. The advantages of the proposed paper has been the best part of the paper. Various functional and non functional requirements are discussed. Finally paper is concluded by mentioning the minimum requirements needed to design the proposed system.

References

[1] Boyang Wang, Baochun Li and Hui Li, "Public auditing for shared data with efficient user Revocation in the cloud", *IEEE Xplore Digital Library, vol 8, Issue 1, Sep 2015.*

[2] Kai He, Chuanhe Huang, Kan Yang and Jiaoli Shi, "Identity-preserving public auditing for shared cloud data," *in the 23rd IEEE International Symposium on Quality of Service (IWQOS), 2015.*

[3] P.Divya and B. Sivananthan, "A Privacy-preserving access control with robust data authenticity for cloud group," *Journal of Scientific and Computational Intelligence, vol. 2, issue 1, Sep 2015.*

[4] G. Shreedevi and K.G. Arunkumar, "Survey of public auditing of shared data with multiple third party auditor with efficient user revocation in cloud" *Journal of Computer Technology and Applications, vol.6 (2), Mar-Apr 2015.*

[5] Prof. Sawan Baghel and Prof. Gaurav Saboo, "Efficient Cryptographic algorithms for cloud storage security," *Journal of Emerging Technologies in Engineering Research, vol.3, issue 2, Nov 2015.*

[6] Aparajitha Sain, Parna Dutta, Namrata Dwivedi, Pradnya Chikhale and Vrunda Bhusari, "Enhancing data storage security in cloud computing using PDDS technique," *Journal of Advanced Research in Computer Engineering and Technology, vol. 4, issue 2, Feb 2015.*

[7] Rushikesh P. Dhanokar and Prof. Gitanjali S. Mate, "Auditing of cloud data with privacy preserving using TPA", *IOSR Journal of Computer Engineering, 2015.*

[8] Mr. Santosh P. Jadhav and Prof. B. R. Nandwalkar, "Efficient cloud computing with secure data storage using AES", *Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue 6, June 2105.*

[9] G. Ranjith, J. Vijaya Chandra, P. Sagarika and B. Prathusha, "Intelligence based Authentication- Authorization and Auditing for secured data storage", *Journal of Advanced in Engineering and Technology, vol. 8, issue 4, Aug 2015.*

[10] Priya Rupeja and Prof. Kalyani Waghmare. "Privacy preserving public auditing and recovery using backup and restore method for secure cloud storage" , *Journal of Engineering and Computer Science, volume. 4, issue 1, Jan 2015.*

[11] Ms. Suvidha R. Sardar and Dr. A. D. Gawande, "Implementation of privacy- preservation in public cloud storage: a Review", *Journal of Advanced Research in Computer Science and Software Engineering, volume 5, issue 4, April 2015.*

[12] Shruti Batham, Umesh Lilhore and Sini Shibu "Improved HLA based encryption process using fixed size aggregate key generation" , *Journal of Modern Trends in Engineering and Research, vol. 2, issue 1, Jan 2015.*

[13] Mehmet SabirKiraz, Isa Sertkaya and Osmanbey Uzunkol, "An Efficient ID-based message recoverable privacy preserving auditing scheme", *in the 13th Annual IEEE Conference on privacy security and trust, 2015.*

[14] Jianhong Zhang and Xubing Zhao, "Privacy- preserving public auditing scheme for shared data with supporting multi function", *Journal of communications, vol. 10, no. 7, July 2015.*

[15] M. Maha Krishna Jeyanthi, P. Muneeswari, M. Nithya and E. Revathi, "Security and privacy for data sharing in a cloud computing using Ring signature", *Journal of Emerging Technology and Innovative Engineering, vol. 1, issue 3, March 2015.*

[16] Franklin Malugu and K. Suresh Babu, "Public audit of cloud shared data by using efficient privacy preserving scheme", *Journal of Scientific Engineering and Research, vol. 3, issue 4, April 2015.*

[17] Kedar Jayesh Rasal, Dr. S. V. Gumaste and Sandip A. Kahate, "Survey on privacy preserving public auditing techniques for shared data in the cloud", *Journal of Engineering Science and Innovative Technology, vol. 4, issue 3, May 2015.*

[18] B. BanuPriya, V. Sobhana and Prof. Mishmala Sushith, "Concise survey on privacy preserving techniques in cloud", *Advanced Research Journal in Science Engineering and Technology, vol. 2, issue 2, Feb 2015.*

[19] Mr. J. Moses Pushparaj and Ms. K. Rekha, "Enhanced Privacy preserving metadata verification by accomplishing traceability for shared data in cloud", *IJAICT, vol. 2, issue 2, June 2015.*

[20] Pooja Kapadne and Deepak Sharma, "Mechanism for privacy preserving public auditing for shared data in cloud", *Journal of Engineering Science and Innovative Technology, vol. 4, issue 5, Sep 2015.*

[21] Guangyang Yang, Hui Xia, Wenting Shen, XiuXiu Jiang and Jia Yu, "Public data auditing with constrained auditing number for cloud storage", *Journal of security and its applications, vol. 9, issue 9, 2015.*

[22] Elakkiya B, Savitha S, Vani Parvathi G, Saranya A and Sindhu S, "Public auditing and data dynamics for cloud storage", *Journal of Computer Science and Engineering Communications, vol. 3, issue 3, 2015.*

[23] Remidicherla Rupa, "Auditing outsourced data on cloud using HLA with random masking technique", *Journal of Engineering Development and Research, vol. 3, issue 3, 2015.*

[24] Dhanya Shenoy and N. P.Chawande, "Privacy preserving secure auditing scheme with split cloud storage", *Journal of Engineering Trends and Technology, vol. 23, no. 4, May 2015.*

[25] Kai He, Chuanhe Huang, Haozhou, Jiaolishi, Xiaomao Wang and Feng Dan, "Public auditing for encryption data with client-side deduplication in cloud storage", *Wuhan University Journal of Natural sciences, vol. 20, issue 4, August 2015.*