ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Enhanced Privacy for Cloud Storage Using Cued Click Points for Regenerating Code

Nikita Naik[1], Renu Suryavanshi[2], Gayatri Shinde[3], Shivani Parmale[4], ProfArchana Kadam[5], Prof Smita Khairnar[6]

Department of Computer Engineering, Pccoe, Savitribai Phule Pune University, India

ABSTRACT: Cloud computing is the term where users can remotely store their data into the cloud so as to enjoy the on-demand various high quality services from a shared pool of configurable computing resources. In cloud storage service, clients upload their data along with authentication information to cloud server. Cloud Server (CS) must prove to a verifier that he is actually storing all of the client's data unchanged. The proposed system focuses on efficient and secured cloud storage system. Our proposed system is introducing TPA (Third party auditor) for verifying the integrity of outsourced storage and dynamic privacy-preserving audit service. It achieves public auditability. In this paper, the proposed system scheme is introducing a public auditing scheme for the regenerating-code-based cloud storage .Proxy server is introduced in proposed scheme to solve the regeneration problem of failed authenticators in the absence of data owners, which is privileged to regenerate the authenticators, into the traditional public auditing system model. Thus, our proposed system is able to completely reduce the online burden of data owners [1].

KEYWORDS: Cloud computing, Cloud storage, Public Auditing, Regeneration-code, TPA.

I. Introduction

Recently, cloud computing is receiving more and more attentions, from both industrial and academic community. Cloud computing separates usage of IT resources from their management and maintenance, so that users can focus on their core business and leave the expensive maintenance of IT services to cloud service provider. However users of outsourced storage are at the mercy of their storage providers for the continued availability of their data.In cloud environment, where all the data are being stored to a centralized server, the trust-worthiness and integrity of data is not that secure. Security in cloud is important because of the growing usage of cloud services for critical data storage and rise in cloud service-specific attacks. Generally the security concerns fall into two broad categories: security issues faced by the cloud service provider and the security issues faced by the customers. The provider must ensure that proper measures have been taken to protect the client's data whereas the client should ensure whether the provider has taken necessary actions to protect their data. In [9] the cloud service providers have to deliver diverse services to many users. They also have to manage the security gradually, since and when they take steps to improve security. This becomes a burden for both the cloud provider and the consumer. So to ensure the privacy and the integrity of the data and to reduce the overhead on the provider and consumer side, a third party auditor has been introduced in the cloud computing domain.

The confidential data hosted in the cloud must be protected by use of both access control and encryption. The third party auditor (TPA), who has expertise and capabilities to conduct public audits on the coded data in the cloud, the TPA is trusted and its audit result is unbiased for both data owners and cloud servers; and a proxy agent, who is semi-trusted and acts on behalf of the data owner to regenerate authenticators and data blocks on the failed servers during the repair procedure. Notice that the data owner is restricted in computational and storage resources compared to other entities and may become off-line even after the data upload procedure. In [2] the proxy, who would always be online, is supposed to be much more powerful than the data owner but less than the cloud servers in terms of computation and memory capacity. To save resources as well as the online burden potentially brought by the periodic auditing and accidental repairing, the data owners resort to the TPA for integrity verification and delegate the reparation to the proxy.

DOI: 10.15680/IJIRCCE.2015. 0405101

In [1] third Party Auditor (TPA) has more capabilities than the user and checks the integrity of data for the user and his audit reports helps the users in evaluating the risk. To fully ensure the data integrity and save the users' computation resources as well as online burden, we propose a public auditing scheme for the regenerating-code-based cloud storage, in which the integrity checking and regeneration are implemented by a third party auditor and a semi-trusted proxy separately on behalf of the data owner. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA.

II. RELATED WORK

In [2], it is mentioned that Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the

Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware software, and personnel maintenances, etc. In [3], it is mentioned that User can upload their data on cloud and can access those data anytime a The proposed scheme focuses on efficient and secure cloud storage system and dynamic privacy-preserving audit service (TPA) for verifying the integrity of outsourced storage. It achieves both public auditability and dynamic data operations anywhere without any additional burden. In [4], there are many things that can motivate the CSP to not behave truthfully towards the user about his outsourced data status. CSP should not use user's data for their own good.

Although the cloud storage architecture is much more secure and powerful then our local computers but then also external and internal threats exist. In [9], it is mentioned that the auditing can be done by the third party without fetching the entire data from the cloud. A data protection scheme is also outlined, by providing a method to allow for data to be encrypted in the cloud without loss of accessibility or functionality for the authorized users**.**

III. EXISTING SYSTEM

The basic system design consists of four entities: The data owner, the cloud storage, the TPA and the user.

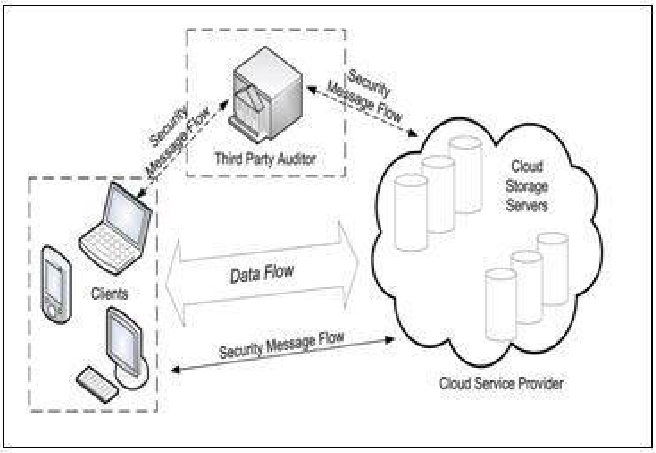

Figure 1. System model.

The data owner is the one who owns large amounts of data files to be stored in the cloud. The *cloud* storage is managed by the cloud service provider who provides storage service and *the third party auditor*(TPA), who has expertise and capabilities to conduct public audits on the coded data in the cloud, the TPA is trusted and its audit result is unbiased for both data owners and cloud servers; and *a proxy agent*, who is semi-trusted and acts on behalf of the data owner to regenerate authenticators and data blocks on the failed servers during the repair procedure. The user downloads the file from cloud through TPA verification.

IV. **PROPOSED SYSTEM**

There are four modules in this project as follows and accordingly they will be implemented:
1. Data User
2. Data Owner
3. TPA
4. Code Generation

1) DATA USER:

The cloud user, who has large amount of data files to be stored in the cloud. Users or data owners, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual's consumers and organizations.

2) DATA OWNER:

It is managed by cloud service provider to provide data storage service and has significant storage space and computation resources. By hosting their data in cloud, data use to store files or data objects. Physically, the resource may span across multiple servers and multiple locations. The safety of the files depends upon the hosting companies, and on the applications that leverage the cloud storage.

3) THIRD PARTY AUDITOR:

TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud. Auditor may be User (Data Owner) or Third Party Auditor. It falls into two categories:

- Private Auditability: allows only data owner for checking the integrity of data file stored on cloud server.

- Public Auditability: allows anyone (not just the client), to challenge cloud server for correctness of data. TPA is honest but curious. It performs whole auditing procedure honestly but it curious about the received data. Thus for the storage of secured data, there also a privacy requirement for third party auditing protocol. The perspective of protecting data privacy, the users, who own the data and rely on TPA just for the storage security of their data, do not want this auditing process introducing new vulnerabilities of unauthorized information leakage toward their data security.

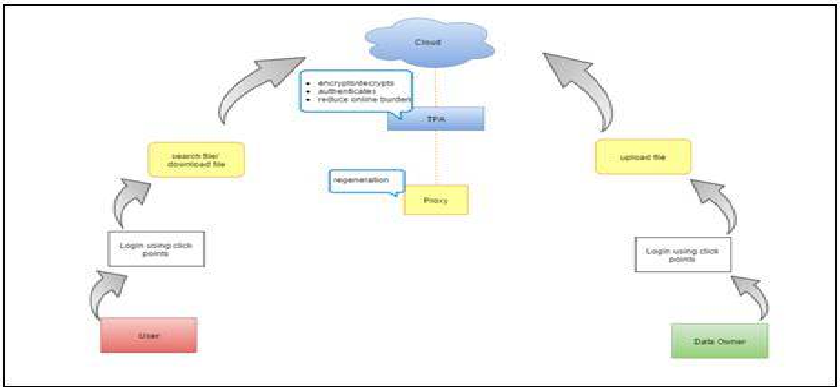

Figure 2. Proposed model

Properties of Proposed system:

- Our system supports public auditability by a TPA.
- Encryption of the file is undertaken prior uploading the same to the cloud server so that no one can gain access its contents.
- Our approach does reduce online burden to users.
- In our approach TPA does not have to maintain results of previous audits.
- This proposed scheme will help in preventing data loss.
- This system will provide more secure access to the user.

3.1 Centered Discretization Algorithm:

The proposed system uses centered discretization graphical password so correct entries are accepted through system. Password is composed of set of clicks on several images. If clicks points are within same grid-square and match with original click points, then entry is accepted as its hash value match with original.

3.1.1 Storing Password

- $i = \lfloor (x - r) / 2r \rfloor$
- $d = (x - r) \bmod 2r$

3.1.2 Password Verification

- $i' = \lfloor (x' - d) / 2r \rfloor$.
- If x' is within tolerance r of x, then $i' = i$ and hence $h(i', d)$ equals the stored value of $h(i, d)$ and system accepts the entry.
- If x' is outside of the accepted tolerance r, it falls in a different segment and $i' \neq i$, thus $h(i', d) \neq h(i, d)$ and the system rejects it.

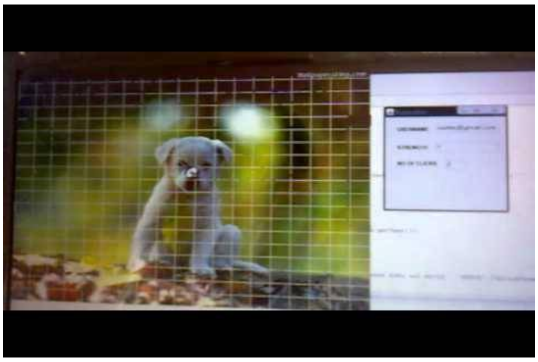

Figure 3. Clicks Points

3.2 Functional Minimum Storage regenerating codes:

FMSR maintains double fault tolerance and eliminate the need to perform encoding operations within storage nodes during repair, while preserving the benefits of network coding in reducing repair traffic. Here we will consider fault tolerant storage based on a type of maximum distance separable (MDS) codes.

Step 1: Given a file object of size M, we divide it into equal size native chunks, which are linearly combined to form code chunks.

Step2: When an (n, k) MDS code is used ,the native/code chunks are then distributed over nodes, each storing chunks of total size M/k, such that the original file object may be reconstructed from the chunks contained in any n-k nodes.

Step3: We call this fault tolerance feature the MDS property.

Step 4: One of the extra feature of FMSR codes is that reconstructing the chunks stored in the failed node can be achieved by downloading less data from the whole file

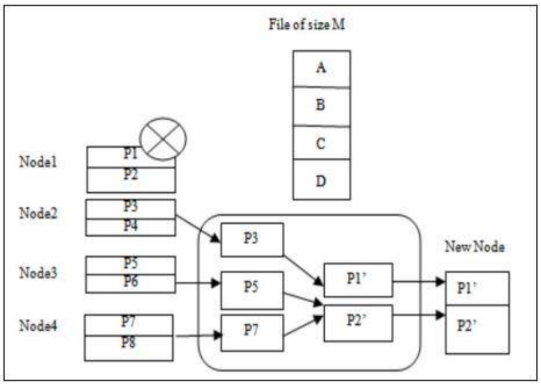

Figure 4. FMSR

V. Results

Work Overhead: Unlike Normal Cloud Storage, our proposed enhanced cloud has TPA reducing the audit work of client.

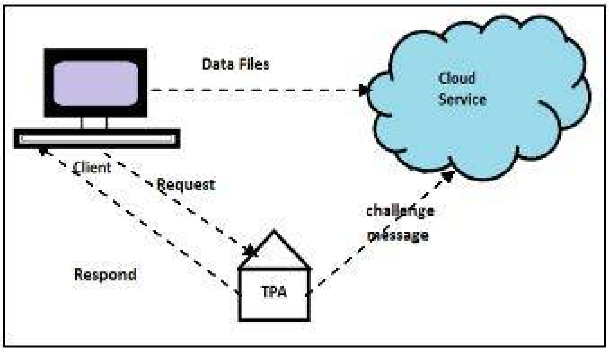

Figure 6.Proposed Enhanced cloud with TPA

DOI: 10.15680/IJIRCCE.2015. 0405101

Description: A cloud data storage service involving three different entities, as shown in figure 6: the cloud user(U),who has large amount of data files to be stored in the cloud; the Cloud Server (CS), which is managed by Cloud Service Provider (CSP) to provide data storage service and has significant storage space and computation resources; the Third Party Auditor(TPA), who has expertise one and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request.

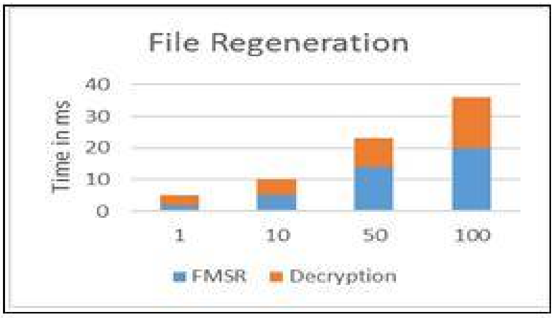

Figure 7. File Regeneration Analysis

Graph shows that the time taken for regeneration which involved both the decoding and decryption using the secret key secured by the proxy server and repair process respectively.

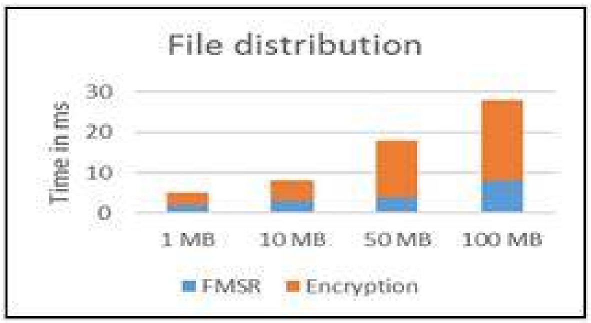

Figure 8. Repair Latency

Graph shows the time taken for both encryption and FMSR encoding process. It is observed that the encryption process takes more time, since it adds more security any cloud provider can afford it.

VI. Conclusion and Future Work

We motivate the public auditing system of the data storage security in cloud computing. Our scheme enables an external auditor to carry out data integrity of the outsourced of the user. We reduce the online burden of the user which supports privacy preserving and public auditing. As cloud computing is a formidable task and user is always in a dilemma about his outsourced data that is when our proposed system extends TPA and proxy server to perform the data integrity task.

The approach discussed in this paper is a way to more advanced research. We can use different algorithm to select multiple pictures from the database for login using click points. Click points presents both challenges and opportunity in future research.

VII. ACKNOWLEDGEMENT

We would like to thank our project guide Prof. Archana Kadam and co-guide Prof. Smita Khairnar for her enormous co-operation and guidance. We have no words to express our gratitude for a person who whole heartedly supported the project and gave freely of her valuable time while making this project. The technical guidance provided by her was more than useful and made the project successful. We would also like to thank our Department of Computer Engineering, Pimpri Chinchwad College of Engineering.

REFERENCES

1. Benjamin C M Fung, Ke Wang, Rui Chen, “Privacy- Preserving Data Publishing: A Survey of Recent Developments, ACM Computing Surveys”, Vol. 42, No. 4, pp.187-198, Article 14, Publication date: June 2010.
2. Bee-Chung Chen, Daniel Kifer, Kristen LeFevre and Ashwin Machanavajjhala, “Privacy-Preserving Data Publishing”, Foundations and Trends in DatabasesVol. 2, Nos. 1–2 (2009) 1–167.
3. K. Yang and X. Jia, “An efficient and secure dynamic auditing protocol for data storage in cloud computing,” Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.
4. A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, “Above the clouds: A berkeley view of cloud computing,” Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, p. 13, 2009.
5. A. 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.
6. C. Wang, Q. Wang, K. Ren, and W. Lou,“Towards secure and dependable storage services in cloud computing,” Service Computing, IEEETransactions on, vol. 5, no. 2, pp. 220–232, May 2012.
7. A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” Information Theory, IEEE Transactions on, vol. 56, no. 9, pp. 4539–4551, 2010.
8. C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp.1-9.
9. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote data checking for network coding-based distributed storage systems,” inProceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010, pp. 31–42.