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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

An Efficient and Secure Dynamic Auditing for Regenerating-Code-Based Cloud Storage

Nareshkumar R.M, Shoaib Zariker

Assistant Professor, Department of Computer Engineering, DYPIEMR, Akurdi, Pune, India[1]

Student, Assistant Professor, Department of Computer Engineering, DYPIEMR, Akurdi, Pune, India[2]

ABSTRACT: To secure outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. Recently, regenerating codes have gained fame due to their lower repair bandwidth while providing fault tolerance. Existing remote checking methods for regenerating-coded data only provide private auditing, requiring data owners to always stay online and handle auditing, as well as repairing, which is sometimes impractical. In this paper, we propose a public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, we introduce a proxy, which is advantaged to regenerate the authenticators, into the conventional public auditing system model. Moreover, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely free data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be possibly integrated into the regenerating code-based cloud storage.

KEYWORDS: Cloud Computing; TPA; Privacy-Preserving; Public Audit;

I. INTRODUCTION

CLOUD storage is now gaining popularity because it offers a flexible on-demand data outsourcing service with attractive benefit free of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personal maintenances, etc., on the other hand this new paradigm of data hosting service also brings new security threats toward users data, thus making individuals or enterprisers still feel doubtful It is noted that data owners lose ultimate control over the fate of their outsourced data; thus, the correctness, availability and integrity of the data are being put at risk [1]. On the one hand, the cloud service is usually faced with a broad range of internal & external adversaries, who would maliciously delete or corrupt users data on the other hand, the cloud service providers may act corruptly, attempting to hide data loss or corruption and claiming that the files are still correctly stored in the cloud for reputation or financial reasons. Thus it makes great sense for users to implement an efficient protocol to perform periodical verifications of their outsourced data to ensure that the cloud indeed maintains their data correctly.

Many mechanisms dealing with the integrity of outsourced data without a local copy have been proposed under different system and security models up to now. The most significant work among these studies are the PDP (provable data possession) model and POR (proof of retrievability) model, which were originally proposed for the single-server scenario by Ateniese et al. [2] and Juels et. al. [3], respectively. Considering that files are usually striped and redundantly stored across multi-servers or multi-clouds, [4]–[10] explore integrity verification schemes suitable for such multi-servers or multi clouds setting with different redundancy schemes, such as replication, erasure codes, and, more recently, regenerating codes.

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 (of failed data blocks and authenticators) are implemented by a third party auditor and a semi-trusted proxy separately on behalf of the data owner. Instead of directly adapting the existing public auditing scheme to the multi-server setting, we design a novel authenticator, which is more appropriate for regenerating codes. Besides, we ”encrypt” the coefficients to protect data privacy against the auditor, which is more lightweight than applying the proof blind technique in and data blind method in . Several challenges and threats spontaneously arise in our new system model with a proxy and security analysis shows that our scheme works well with these problems.

A. *Problem Statement*

Recently, regenerating codes have gained fame due to their lower repair bandwidth while providing fault lack of complaint Existing remote checking methods for regenerating-coded data only provide private auditing, requiring data owners to always stay online and handle auditing, as well as repairing, which is sometimes impractical. In this paper, we recommend a public auditing scheme for the regenerating-code-based cloud storage.

B. *Objectives*

1. Input Design is the process of converting a user-oriented report of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating easy to use screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and free from errors.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant.

C. Existing system

We focus on the reliability verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy extended the single-server CPOR scheme (private version in) to the regenerating code-scenario designed and implemented a data integrity protection scheme for FMSR based cloud storage and the scheme is adapted to the thin-cloud setting. However, both of them are designed for private audit, only the data owner is allowed to verify the integrity and repair the faulty servers. Considering the large size of the outsourced data and the user’s constrained resource capability, the tasks of auditing and reparation in the cloud can be difficult and expensive for the users. The overhead of using cloud storage should be minimized as much as possible such that a user does not need to perform too many operations to their outsourced data. In particular, users may not want to go through the complexity in verifying and reparation. The auditing schemes imply the problem that users need to always stay online, which may slow down its approval in practice, especially for long-term archival storage.

Disadvantages:

- Remote checking methods for regenerating-coded data only provide private auditing,
- Requiring data owners to always stay online and handle auditing, as well as repairing
- It is noted that data owners lose ultimate control over the fate of their outsourced data

II. Related work

Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu , Proposed, cooperative PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy. Also proved the security of based on multiprover zero-knowledge proof system, which can satisfy completeness, knowledge soundness, and zero-knowledge properties. They had a problem of Provable data possession (PDP), it is a technique for ensuring the integrity of data in storage outsourcing. It address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. However, they proposed cooperative PDP (CPDP) scheme [10].

C.Wang, S.S.Chow, Q.Wang, K.Ren,and W.Lou, proposed a secure cloud storage system supporting privacy-preserving public auditing for a problem of using cloud storage. Users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public audit ability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worrying free [11].

A. G. Dimakis et al. for distributed storage to reduce the repair bandwidth. Viewing cloud storage to be a collection of n storage servers, data file F is encoded and stored redundantly across these servers. Then F can be retrieved by connecting to any k-out-of-n servers, which is termed the MDS2-property. When data corruption at a server is detected, the client will contact ℓ healthy servers and download β' bits from each server, thus regenerating the corrupted blocks without recovering the entire original file. Dimakis showed that the repair bandwidth $\gamma' = \ell\beta'$ can be significantly reduced with $\ell \geq k$. Furthermore, they analyzed the fundamental tradeoff between the storage cost α' and the repair bandwidth γ', then presented two extreme and practically relevant points on the optimal tradeoff curve: the minimum bandwidth regenerating(MBR)point, which represents the operating point with the least possible repair bandwidth, and the minimum storage regenerating(MSR) point, which corresponds to the least possible storage cost on the servers [12].

III. PROPOSED SYSTEM

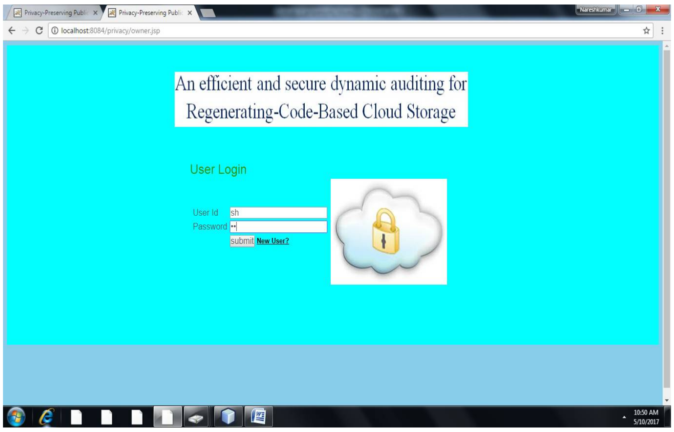
We propose a public auditing scheme for the regenerating-code-based cloud storage, in which the integrity checking and regeneration (of failed data blocks and authenticators) are implemented by a third-party auditor and a semi-trusted proxy separately on behalf of the data owner. Instead of directly adapting the existing public auditing scheme to the multi-server setting, we design a novel authenticator, which is more appropriate for regenerating codes. Besides, we" encrypt" the coefficients to protect data privacy against the auditor, which is more lightweight than applying the proof blind technique and data blind method. Several challenges and threats spontaneously arise in our new system model with a proxy and security analysis shows that our scheme works well with these problems.

Advantages:

- We design a novel homomorphic authenticator based on BLS signature, which can be generated by a couple of secret keys and verified publicly.
- To allow privacy-preserving public auditing for regenerating code-based cloud storage. The coefficients are masked by a PRF (Pseudorandom Function) during the Setup phase to avoid leakage of the original data.
- Our scheme completely releases data owners from online burden for the regeneration of blocks and authenticators at faulty servers and it provides the privilege to a proxy for the reparation.
- Optimization measures are taken to improve the flexibility and efficiency of our auditing scheme; thus, the storage overhead of servers, the computational overhead of the data owner and communication overhead during the audit phase can be effectively reduced.

IV. RESULTS AND DISCUSSIONS

Figure 1 &2, shows the user login page, before logging in to the system security code will be sent to user registered email id. After entering that code user allows to enter in to the system.



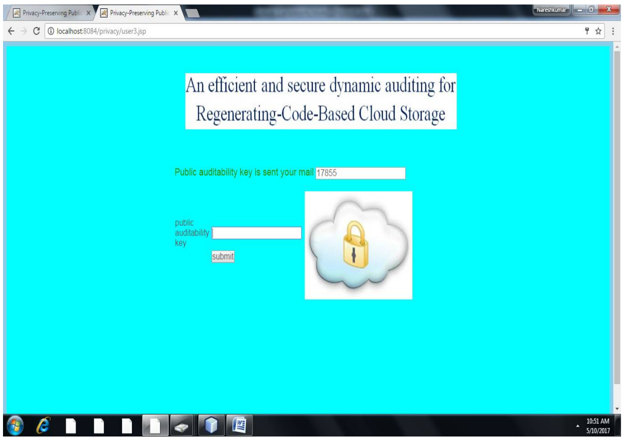
localhost:8084/privacy/owner.jsp

An efficient and secure dynamic auditing for Regenerating-Code-Based Cloud Storage

User Login

User Id: sh
Password: ••

Figure-1: User Login Page



localhost:8084/privacy/user3.jsp

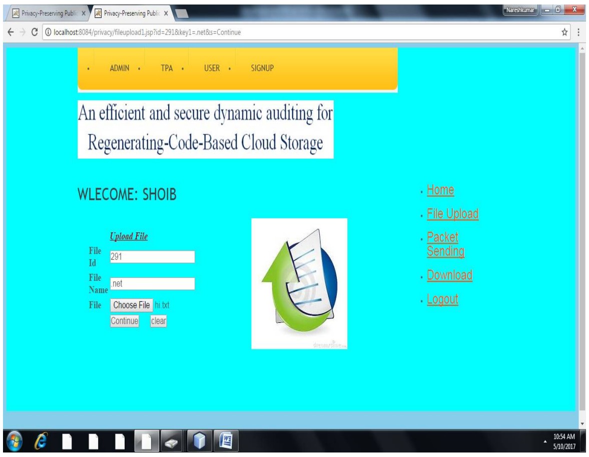
An efficient and secure dynamic auditing for Regenerating-Code-Based Cloud Storage

Public auditability key is sent your mail: 17855

public auditability key:

Figure-2: Key Generating on Registered Email

Figure 3 & 4, represents uploading a file in to the cloud and dividing data in to the number of sections as blocks available. Code will be generated for each block.



localhost:8084/privacy/fileupload1.jsp?id=291&key1=.net&s=Continue

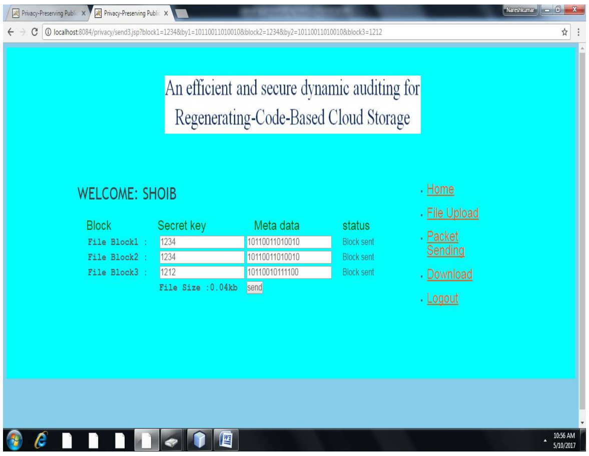
An efficient and secure dynamic auditing for Regenerating-Code-Based Cloud Storage

WLECOME: SHOIB

Upload File

File Id: 291
File Name: net
File: Choose File hi.txt

Figure-3: File Upload Page



localhost:8084/privacy/send3.jsp?block1=1234&by1=10110011010010&block2=1234&by2=10110011010010&block3=1212

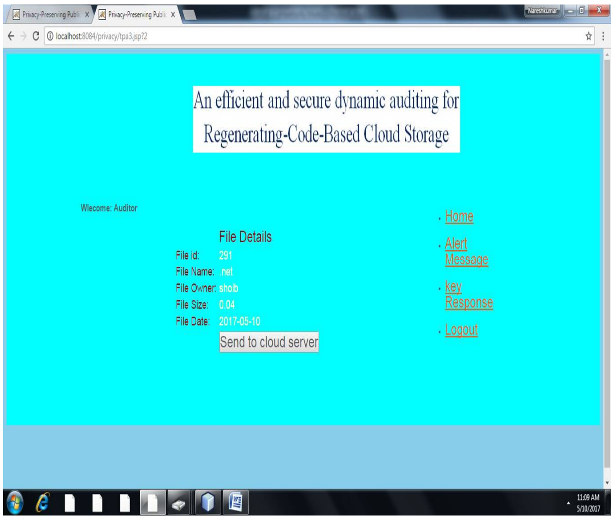
An efficient and secure dynamic auditing for Regenerating-Code-Based Cloud Storage

WELCOME: SHOIB

Block	Secret key	Meta data	status
File Block1 :	1234	10110011010010	Block sent
File Block2 :	1234	10110011010010	Block sent
File Block3 :	1212	10110010111100	Block sent
	File Size :0.04kb	send	

Figure-4: Multiple Key Generating for Packet

Figure 5 & 6 indicates, once generate the code for each block, and next send uploaded file to cloud. Then verify the file in cloud and send to TPA for integrity and allow the accessibility.



localhost:8084/privacy/tpa3.jsp?2

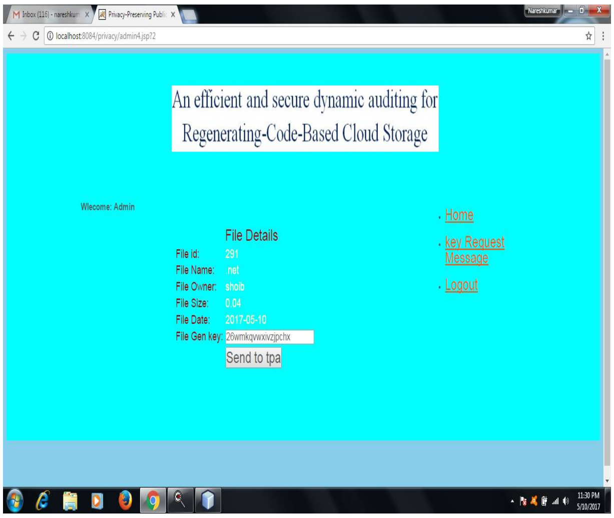
An efficient and secure dynamic auditing for Regenerating-Code-Based Cloud Storage

Wlecome: Auditor

File Details

File id: 291
File Name: .net
File Owner: shoib
File Size: 0.04
File Date: 2017-05-10

Figure-5: Verifying file from TPA to Cloud Security



localhost:8084/privacy/admin4.jsp?2

An efficient and secure dynamic auditing for Regenerating-Code-Based Cloud Storage

Wlecome: Admin

File Details

File id: 291
File Name: .net
File Owner: shoib
File Size: 0.04
File Date: 2017-05-10
File Gen key: 26wmkqvwxivzjpchx

Figure-6: Generating Key for File to TPA

V. Conclusion

We propose a secure public auditing system for data storage security in Cloud Computing. We utilize the random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the boring and possibly expensive auditing task, but also alleviate the users fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our secure public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

REFERENCES

1. Nareshkumar R.M, Gayatri Sarag and Pooja Doshi, "Privacy-Preserving Public Auditing Data Integrity For Shared Data In The Cloud ", International Journal of Research In Science & Engineering , Volume: 1 Issue: 6, pp.61-64, 2015.
2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, pp. 598– 609, 2007.
3. A. Juels and B. S. Kaliski Jr, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, pp. 584–597, 2007.
4. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "Mr-pdp: Multiplereplica provable data possession," in Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on. IEEE, pp. 411–420, 2008.
5. K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in Proceedings of the 16th ACM conference on Computer and communications security. ACM,pp. 187–198, 2009.
6. J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographicallydispersed clouds," Journal of Computer and System Sciences, vol. 78, no. 5, pp. 1345–1358, 2012.
7. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote data checking for network coding-based distributed storage systems," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, pp. 31–42, 2010.
8. H. Chen and P. Lee, "Enabling data integrity protection in regeneratingcoding-based cloud storage: Theory and implementation," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 407–416, Feb 2014.
9. 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.
10. Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 12, pp. 2231– 2244, 2012.
11. C.Wang,S.S.Chow,Q.Wang,K.Ren,andW.Lou,"Privacy-preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.
12. A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," Proceedings of the IEEE, vol. 99, no. 3, pp. 476–489, 2011.

BIOGRAPHY

Mr. Nareshkumar R. Mustary, working as a Assistant Professor in Dr.D.Y.Patil Institute of Engineering, Management & Research, Akurdi, Pune. Completed Bachelor of Engineering (computer science & Engineering) from Rural Engineering College, Bhalki, affiliated to Visveshvaraiah Technological University, Belgaum, Karnataka with First class with distinction (74%) in 2008, Master of Technology (Software Engineering) from Al-Habeeb College of Engineering, Hyderabad with first class with distinction (76%) in 2012 & Pursuing PhD from GITAM, University, Hyderabad. I have published 9 papers in different International Journals and presented in 5 International and National conferences. My research areas of interests are: Ad-hoc Networks, Mobile Computing, Artificial Intelligence, and Design of Algorithm.