INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue2)
Available online at www.ijariit.com

Privacy Preserving and Secure Data Integrity Protection security in Regenerating Coding Based Public Cloud Storage

Monika B. Thakare
Computer Science & Engineering,
RTMNU University, A.C.E, Wardha, Maharashtra, India
thakare.monika894@gmail.com

Prof. N. M. Dhande
Computer Science & Engineering,
RTMNU University, A.C.E, Wardha, Maharashtra, India
nutandhande@yahoo.com

Abstract : Now a day's use of cloud computing is rapidly increasing. Cloud infrastructure is being a common solution adopted by large organizations for storing and accessing data. It provides the current need for data storage with a flexible and dynamic storage that can grow. In this paper, we describe the design and development of a cloud computing based secure cloud data storage using encryption. Cloud data storage is a major solution to overcome this problem. These mechanisms to provide data integrity and security for client's data in cloud storages. In users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. This understands the trend in terms of complexity and strength of a secured solution and provides some insights of what is still left in such area of research. Cloud data storage provide better privacy as well as ensure data availability and reliability can be achieved by dividing the user's data block into data pieces. 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 worry-free.

Keywords: Cloud Storage, Privacy Preserving, Public Auditing, Data Integrity.

I. INTRODUCTION

Cloud computing resources can be quickly extracted with all the processes, services and applications provisioned on demand service despite the consequences of the user location or device. Many small scale businesses and organization can establish its infrastructure without the need for implementing actual hardware and software that are needed to build the entire structure as it can entirely rely on the cloud services and use its resources on pay per use basis. The use of cloud computing service provides fast access the Applications and reduces service costs. Cloud computing is being very popular and largely separated especially with the increased usage of internet connectively and virtualization techniques. Every cloud users want to avoid untreated cloud provider for personal and important documents such as debit/credit cards details or medical report from hackers or malicious insiders is the importance. A cluster of cloud storage is created and maintained to satisfy the user specific data access requirements. The beauty of cloud computing is won't need to buy equipment to use the services. Cloud service providers to provide security, but cannot provide data integrity and security in all cases. As a result, the correctness of the data in the cloud is being at risk due to the following reasons. First, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats to data integrity. And second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status. To protect Outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. Public auditing scheme is for the regenerating-code-based cloud storage.

II.LITERATURE REVIEW

1. Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage [1]
In this paper author, it proposed two schemes first for auditing scheme and second for privacy preserving. It proposed public auditing scheme which allows the public verifier to audit the correctness of data even in which the data owner is offline. They proposed the data owner is able to generate those authenticators in a new method, which is more efficient compared to the straightforward approach.

2. Enabling Data Integrity Protection In Regenerating-Coding-Based Cloud Storage: Theory and Implementation[2]

In this paper, Henry C.H. Chen implements the DIP scheme which is designed under a mobile and enable the client to feasibly verify the integrity of random subsets of outsourced data. It works under the simple assumption of thin-cloud storage and allows different parameters.

3. NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds[3]

This paper author implements an auditing framework for cloud storage systems and it proposes an efficient and privacy-preserving auditing protocol, further extended auditing protocol to support the data operation. It also checks the correctness of the data operation. It implements batch auditing for both multiple owners and multiple clouds.

4. An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing [4]

This paper the author focuses on an auditing framework for cloud storage systems and proposes an efficient and privacy-preserving auditing protocol, further extended auditing protocol to support the data dynamic operation. The further extend auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer.

5. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing[6]

In this paper author focus on a combination the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system. It supports efficient handling of multiple auditing tasks. They explorer TPA can perform multiple auditing tasks simultaneously.

6. Distributed data possession checking for securing multiple replicas in geographically dispersed clouds [6]

In this paper, the author will help it provide a novel efficient Distributed Multiple Replicas Data Possession Checking (DMRDPC) scheme to tackle new challenges. It also will help the cloud users to achieve efficient multiple replicas data possession checking. It is important to ensure that each replica should have availability and data integrity features. In this paper, Remote data possession checking is a valid method to verify the replica's availability and integrity.

7. Toward secure and dependable storage services in cloud computing [7]

In this paper author proposed a flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed erasure-coded data. It proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append**.** It proposed scheme is highly efficient and resilient against malicious data modification attack and even server colluding attacks.

8. Secure and efficient privacy-preserving public auditing scheme for cloud storage[8]

In this paper, the author proposes a new privacy-preserving public auditing mechanism for shared data in an untrusted cloud. Here, It utilizes ring signature so that the third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the TPA. This paper provides a privacy-preserving public auditing scheme that supports public auditing and identity privacy on shared data stored in the cloud storage service for enhancing its security and efficiency.

9. Network coding for distributed storage systems[9]

In this paper, the author introduces a general technique to analyze storage architectures that combine any form of coding and replication, as well as presenting two new schemes for maintaining redundancy using erasure codes. It shows how network coding can help for such distributed storage scenarios.

10. A survey on network codes for distributed storage[10]

In this paper, the author proposed the demand for large-scale data storage has increased significantly, with applications. The peer-to-peer networks, redundancy must be introduced into the system to improve reliability against node failures. It realizes the increased reliability of coding, however, one has to address the challenge of maintaining an erasure encoded representation.

11. NCCloud: Applying network coding for the storage repair in a cloud-of-clouds[11]

In this paper author proposed cloud storage provides an on-demand remote backup solution. To provide fault tolerance for cloud storage to proposed data across multiple cloud vendors. It preserves data redundancy. It implements a proof-of-concept prototype of NCCloud and deploys it atop both local and commercial clouds.

12. HAIL: A high-availability and integrity layer for cloud storage[12]

In this paper author proposed HAIL a distributed cryptographic system that permits a set of servers to prove to a client that a stored file is intact and retrievable.HAIL cryptographically verifies and reactively reallocates file shares. It explores a unification to remote file-integrity assurance in a system that calls HAIL (High-Availability and Integrity Layer).

13. Enhancing Security and Privacy in Multi-Cloud Computing Environment[13]

In this paper authors implement the cloud computing is a cost-effective, service availability, flexible and on-demand service delivery platform for providing business through the internet. It is a form of secret sharing.The use of cloud computing for many reasons including because this service provides fast access the Applications and reduce service costs.

14. Security Approach for Multi-Cloud Data Storage[14]

In this paper author proposed transformation of information and storage of sensitive data has the highest priority. A cluster of cloud storage is created and maintained accordingly to satisfy the user specific data access requirements. It is important to ensure that each replica should have availability and data integrity features.

15. A Privacy Manager for Cloud Computing[15]

In this paper author proposed it describes a privacy manager for cloud computing, It also describes how Trusted Computing mechanisms can optionally be used to enhance privacy management. The result of the processing is by the privacy manager to reveal the correct result.

III. COMPARATIVE STUDY OF LITERATURE SURVEY

SR. NO	NAME OF PAPER	YEAR	AUTHOR	DESCRIPTION
1	Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage.	April-2015	Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian	It used first auditing scheme and second for privacy preserving.
2	Enabling Data Integrity Protection In Regenerating-Coding-Based Cloud Storage: Theory and Implementation	July-2014	Henry C.H. Chen and Patrick P.C. Lee	It used DIP scheme which is designed under a mobile and enables a client to feasibly verify the integrity.
3	NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds	June- 2014	B. P. Jackson, A. A. Goshtsaby	It checks the correctness of the data operation. It implements batch auditing scheme.
4	An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing	May -2013	Kan Yang, Xiaohua Jia,	It used auditing framework for cloud storage systems and proposes an efficient and privacy-preserving auditing protocol.
5	Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing	May-2010	Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou.	It used public key based homomorphic authenticator for security**.**
6	Distributed data possession checking for securing multiple replicas in geographically dispersed clouds	September-2012	J.He, Y. Zhang, G. Huang, Y. Shi, and J. Cao.	It provides a novel efficient Distributed Multiple Replicas Data Possession Checking (DMRDPC) scheme to tackle new challenges.
7	Toward secure and dependable storage services in cloud computing	April/june2012	C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou	It designs secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append**.**
8	Secure and efficient privacy-preserving public auditing scheme for cloud storage	January-2013	S. G. Worku, C. Xu, J. Zhao, and X. He.	It utilizes ring signature so that the third party auditor is able to verify the integrity of shared data for a group of users.
9	Network coding for distributed storage systems	September-2010	A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran.	Introduce a general technique to analyze storage architectures that combine any form of coding and replication.
10	A survey on network codes for distributed storage	March-2011	A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh.	It realizes the increased reliability of coding**.**
11	NCCloud: Applying network coding for the storage repair in a cloud-of-clouds	March-2012	Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang.	It provides an on-demand remote backup solution. To provide fault tolerance.
12	HAIL: A high-availability and integrity layer for cloud storage	December 2009	K. D. Bowers, A. Juels, and A. Oprea.	It retrievable. HAIL cryptographically verifies and reactively reallocates file shares.
13	Enhancing Security and Privacy in Multi-Cloud Computing Environment	May-2007	Hassan Takabi, James B.D., Joshi, Gail-Joon, Ahn,	It provides fast access the Applications and reduces service costs.

14	Security Approach for Multi-Cloud Data Storage	September-2015	Mohammed A. AlZain, Ben Soh, Eric Pardede,	A cluster of cloud storage is created and maintained accordingly to satisfy the user specific data access requirements.
15	A Privacy Manager for Cloud Computing	June-2008	R. Curtmola, O. Khan, R. Burns, and G. Ateniese,	Trusted Computing mechanisms can optionally be used to enhance privacy management.

IV.PROBLEM DEFINITION

- Regenerating codes have recently been proposed to minimize repair traffic.
- The auditing schemes imply the problem that users need to always stay online.
- It fully ensures the data integrity and saves the user's computation resources as well as an online burden.

V. MODULE

- Implementation of Privacy-Preserving Public Auditing Module.
- Implementation Data Dynamics Module.
- Implementations of Proxy sever.

a) Implementation of Privacy-Preserving Public Auditing Module.

- **ECDSA - Elliptic Curve Digital Signature Algorithm**

Signature Generation:

For signing a message m by sender A, using A's private key d_A
and public key $Q_A = d_A * G$

1. Calculate e = HASH (m), where HASH is a cryptographic hash function, such as SHA-1
2. Select a random integer k from [1,n − 1]
3. Calculate $r = x_1 \pmod n$, where $(x_1, y_1) = k * G$. If r = 0, go to step 2
4. Calculate $s = k^{-1}(e + d_A r) \pmod n$. If s = 0, go to step 2
5. The signature is the pair (r, s)

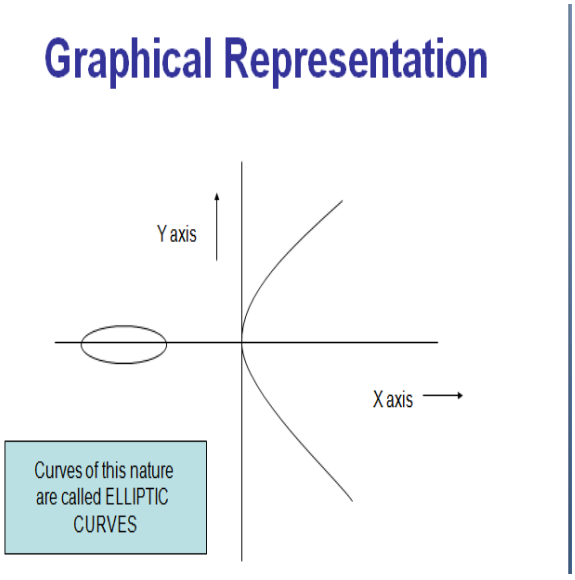
- **ECDSA - Elliptic Curve Digital Signature Algorithm**

Signature Verification:

For B to authenticate A's signature, B must have A's public key Q_A

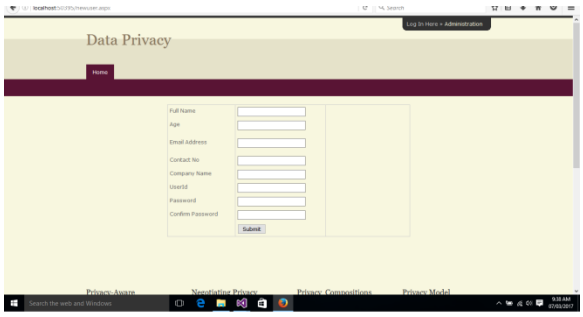
1. Verify that r and s are integers in [1,n − 1]. If not, the signature is invalid
2. Calculate e = HASH (m), where HASH is the same function used in the signature generation
3. Calculate $w = s^{-1} \pmod n$
4. Calculate $u_1 = ew \pmod n$ and $u_2 = rw \pmod n$
5. Calculate $(x_1, y_1) = u_1 G + u_2 Q_A$
6. The signature is valid if $x_1 = r \pmod n$, invalid otherwise

GRAPHICAL REPRESENTION OF ECC



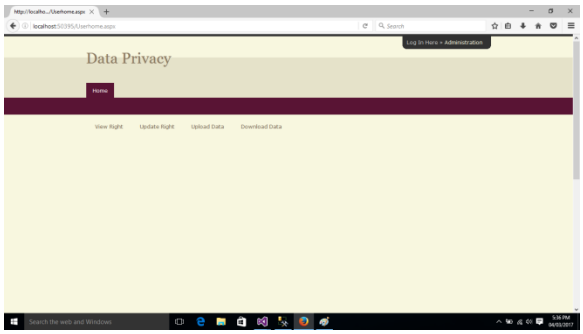
b) IMPLEMENTATION DATA DYNAMICS MODULE.

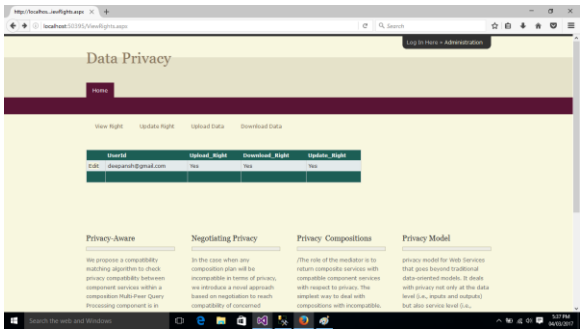
The first step in which the new user fist register then login.

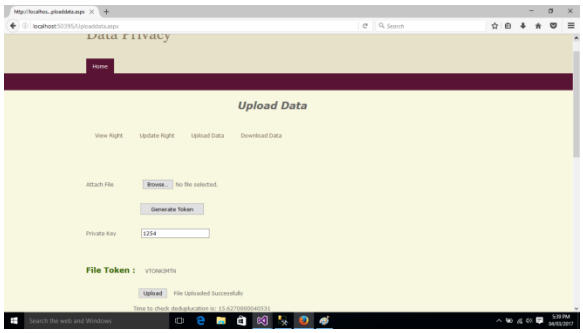


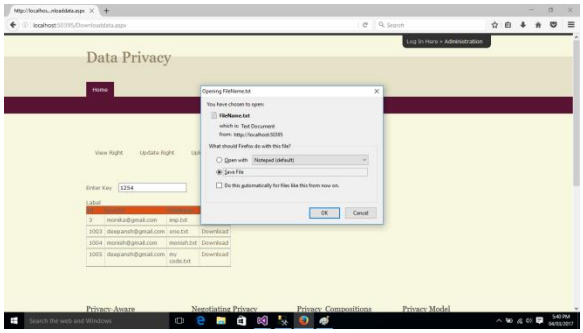
It's a log in page which user is already registered that user login.

From this page, we can see the user right which able to upload or download the data from the server.



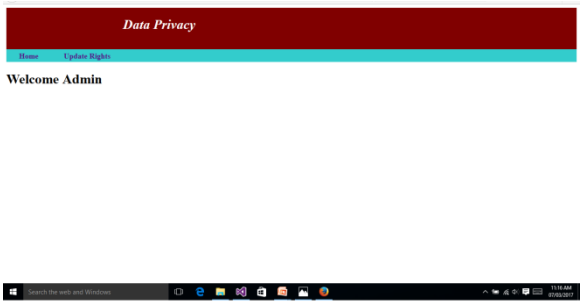


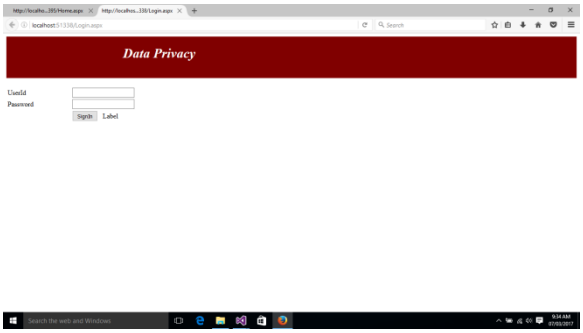




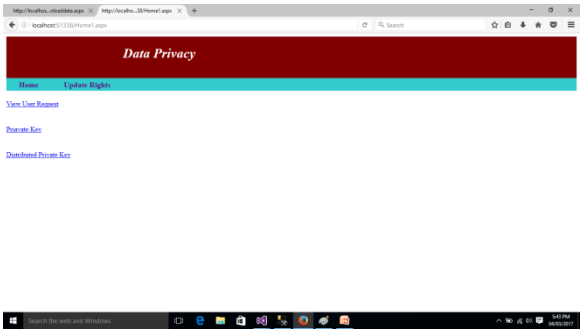
c) IMPLEMENTATION OF PROXY SERVER.

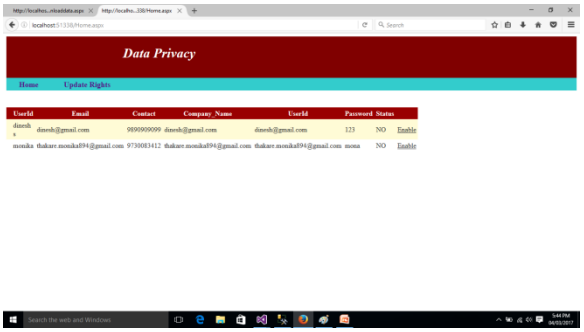
This shows admin which having all rights



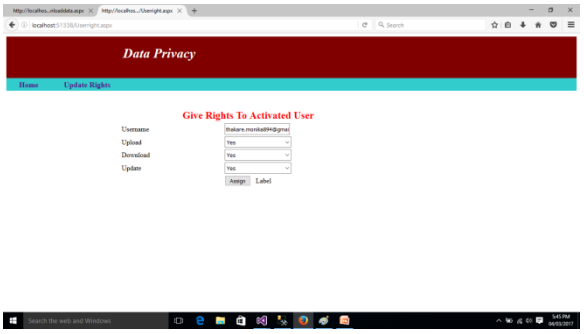


Here shows all users requests.

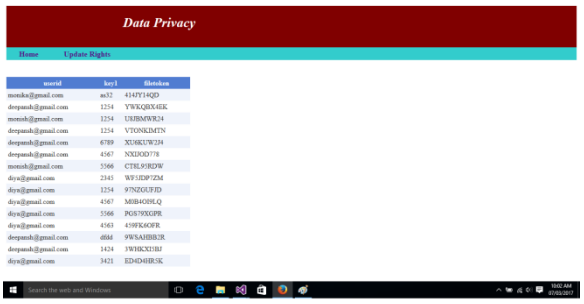




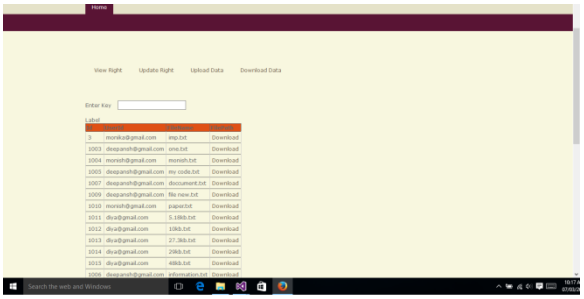
After the user request assigns the rights as per user request.



Token will be generated for each file.



The encrypted file can be downloaded from this page.



VI.OBJECTIVE

The main objectives of the study are listed below:

- To calculate the time of communication of cloud data storage.
- To generate the security for the TPA.
- To provide the execution time of encryption and decryption for security analysis.
- To Performing Comparative time of computation.

VII. PROPOSED SYSTEM

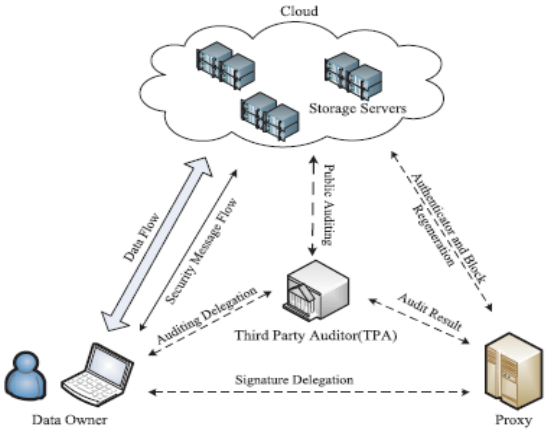


Fig: Cloud Regeneration System Architecture

In this paper focus on the integrity verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy as shown in Fig.1.The proposed system contains the cluster of cloud storages. It may call as "Cloud of clouds" or "multi-clouds". These individual clouds are interconnected to each other. Here, the user uploaded file is replicated on more than one cloud storage that is two to three different interconnected but individual clouds. Our system assigns a unique number to the file which is used by to generate the set of secret keys. The auditing system model for Regenerating-Code-based cloud storage as which consist of four blocks: data owner which consist of large amount of data stored in the cloud; the cloud, which provides cloud services; provide storage service and have significant computational resources; the third party auditor (TPA) conducts public audits on the coded data in the cloud, its audit results are unbiased for both data owner and cloud servers; and 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 proxy is supposed to be much more powerful than the data owner but less than the cloud servers in terms of computation and memory capacity, who would be always online. The data owners to the TPA for integrity verification and delegate the reparation to the proxy. 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.

CONCLUSION

In this paper, it presents a public auditing scheme for the regenerating-code-based cloud storage system, where the data owners are privileged to delegate TPA for their data validity checking. To provide security to the original data privacy against the TPA, It randomizes the coefficients in the starting rather than applying the blind technique within the auditing process. Assuming that data owner is not always able to stay online in practice, in order to keep storage available and verifiable after malicious corruption, we introduce semi trusted proxy into the system model and provide a privilege for proxy to handle the reparation of coded block and authenticators. Thus, this authenticator can be efficiently generated by the data owner simultaneously with encoding procedure.

REFERENCES

[1] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, "Privacy Preserving Public Auditing for Regenerating-Code-Based Cloud Storage", 2015.
[2] Henry C.H. Chen and Patrick P.C. Lee, "Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation", 2014.
[3] Henry C.H. Chen, Yuchong Hu, Patrick P.C. Lee, and Yang Tang, "NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds", 2014.
[4] Kan Yang, Xiaohua Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", 2013.
[5] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, and Mengyang Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage", 2012.
[6] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", 2010.
7] J.He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographically dispersed clouds," J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1345–1358, 2012.

[8] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," Apr./Jun. 2012.
[9] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy preserving public auditing scheme for cloud storage", 2013.

[10] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," Sep. 2010.
[11] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231–2244, Dec. 2012.
12] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," Proc. IEEE, vol. 99, no. 3, pp. 476–489, Mar. 2011
[13] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2008, pp. 90–107.
[14] Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, "NCCloud: Applying network coding for the storage repair in a cloud-of-clouds," in Proc. USENIX FAST, 2012, p. 21.
[15] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.
[16] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.
[17] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 598–609.
[18] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th
ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.
[19] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in Proc. 28th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2008, pp. 411 420.
[21] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," in Proc. 16th ACM Conf. Comput. Commun. Secur., 2009, pp. 187–198.
[22] J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographicallydispersed clouds," J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1345–1358, 2012.
[23] S. Subashini, V.Kavitha, "A Surveys on Security and privacy Issues invService Delivery Models of the Cloud Computing", Journal of Networks and Computer Applications, 34 (1), 2011, pp1-11.
[24] Dawson, E.; Donovan, D. (1994), "The breadth of Shamir's secretsharing scheme", Computers & Security 13: 69–78
[25] Cloud Computing Security: From Singleto Multi-Clouds, 2012, 45th Hawaii International Conference on System Sciences
[26] Md. TanzimKhorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi, "A surveys on gaps, threat remediation challenge, and some thoughts for proactive attack detection in the cloud computing", School of Information and Communication Technology, CQ University QLD 4702, Australia. Received 15 August 2011. Revised 11 January 2012. Accepted 18 January 2012. Available online 27 January 2012.
[27] C. Cachin, I. Keidarand A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
[28] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.
[29] Review of methods for secret sharing in cloud Computing- "International Journal of Advanced Research in Computer Engineering & Technology IJARCET)", Volume 2, Issue 1,
January 2013
[30] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology. Berlin, Germany: Springer Verlag, 2001, pp. 213–229.
[31] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," IEICE Trans. Fundam. Electron., Commun., Comput. Sci., vol. E84-A, no. 5, pp. 1234–1243, 2001.
[32] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin, "Secure network coding over the integers," in Public Key Cryptography. Berlin, Germany:
Springer-Verlag, 2010, pp. 142–160.
[33] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature schemesecure against adaptive chosen-message attacks," SIAM J. Comput.,
vol. 17, no. 2, pp. 281–308, 1988.

