World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 259-265
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Monika B Thakare
Computer Science & Engineering, RTMNU University, A.C.E, Wardha, Maharashtra, India

N. M. Dhande
RTMNU University, A.C.E, Wardha, Maharashtra, India

Correspondence:
Monika B Thakare
Computer Science & Engineering, RTMNU University, A.C.E, Wardha, Maharashtra, India

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

Monika B Thakare, N. M. Dhande

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 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

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 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 increase 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. 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 for 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.

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 implement the DIP scheme which is designed under a mobile and enable 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 implement an auditing framework for cloud storage systems and it propose 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 implement 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 is focus 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 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 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 author propose a new privacy preserving public auditing mechanism for shared data in an untrusted cloud. Here, It utilize 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 author introduce 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 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. 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 provide fast access the Applications and reduce service costs.

Compatative Study of Literature Survey

SR.NO	Technique	Concept	Strength	Weakness
1	It uses method regenerating-coded data only provide private auditing. And also AES encryption technique.	A public auditing scheme for the regenerating-code-based cloud storage.	It is the first to allow privacy-preserving public auditing for regenerating code- based cloud storage.	They are designed for private audit, only the data owner is allowed to verify the integrity and repair the faulty servers.

2	It implements and evaluates the overhead of DIP scheme for much database replication technique.	To protect the outsource data in cloud storage against corruption adding fault tolerance to cloud storage.	A thin-cloud setting is used where servers only need to support standard read/write functionalities for portability and simplicity.	A major limitation in the existing system is that they are designed for a single-server setting.
3	It uses the inverse matrix decipher for creating inverse.	It construct the new data pieces and write these new pieces in FMSR code.	A Highly available cloud storage service with strong consistency.	It may not be flexible for some storage devices.
4	Remote integrity checking method can be used only for static archive data.	In cloud computing data owner host their data server and users can access the data from cloud.	Provide maximum secureness for the user's data.	The TPA cannot derive user's Data from information during auditing.
5	Provable the data possession (PDP) technique used for integrity of data.	Verify the protocol for secure out storing in multicloud environment	The scheme should provide adequate security features to resist some existing attacks, such as data leakage attack and tag forgery Attack.	It used public key based homomorphic authenticator for security.
6	It provides a novel efficient Distributed Multiple Replicas Data Possession Checking (DMRDPC) scheme to tackle new challenges.	Multiple replicas in geographically dispersed.	It has the strong of high scalability, ease of use, cost effectiveness, and so on.	Distributed data possession checking for securing multiple replicas in geographically dispersed clouds.
7	It uses the cloud service provider.(CSP)	Which store the data resources, software and data information for verification protocol.	To ensure the security and dependencies for cloud.	In case user forgot where the data stored, it will become difficult for users.
8	Homorphic AES algorithm.	It has mainly concentrated on improving the security.	Sensitive data has highest priority.	Available the data to the right person or users.
9	Minimum bandwidth regenerating code technique.(MBR)	Network coding for distributed system	It uses peer to peer distributed system.	It used lower bandwidth.
10	Network coding technique can use for addressing.	To repair the network traffic and raise the new challenges.	Improve the reliability and use the redundancy for straightforward of multiple storage node.	Each storage node can store multiple sub-packets.

Problem Definition

A unique problem introduced during the process of public auditing for shared data in the cloud is how to preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a higher valuable target than others. However, no existing mechanism in the literature is able to perform public auditing on shared data in the cloud while still preserving identity privacy. It proposed a new privacy preserving public auditing mechanism for shared data in an untrusted cloud. Here, we utilize 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. The cryptographic storage system that enables secure file sharing on un-trusted servers. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys.

- 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 save the users computation resources as well as online burden.

Module

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

I.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

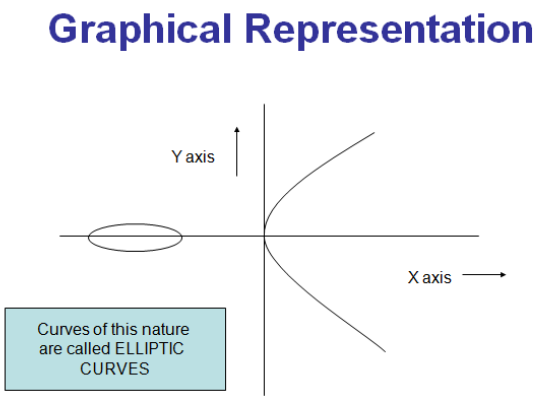
Signature Verification:

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

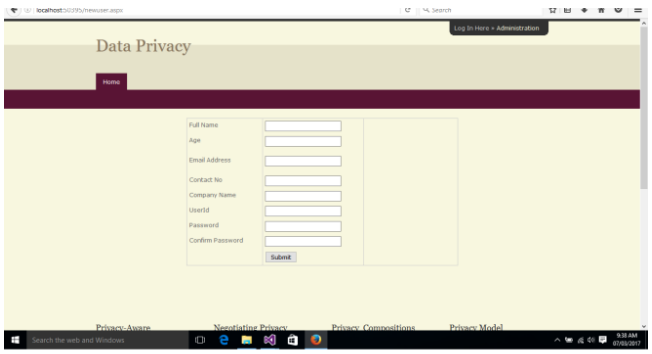
1. Verify that r and s are integers in [1,n − 1]. If not, the signature is invalid
2. Calculate e = HASH (m), where HASH is the same function used in the signature generation
3. Calculate $w = s^{-1} \pmod n$

4. Calculate $u_1 = ew \pmod n$ and $u_2 = rw \pmod n$
5. Calculate $(x_1, y_1) = u_1G + u_2Q_A$
6. The signature is valid if $x_1 = r \pmod n$, invalid otherwise

Graphical Represention of ECC

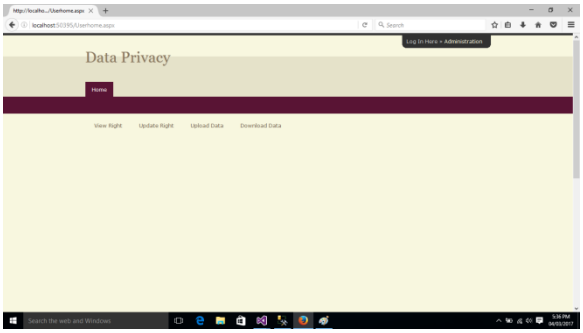


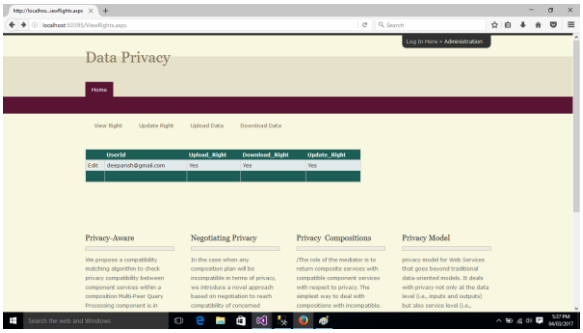
II. Implementation Data Dynamics Module.
The first step in which the new user fist register then log in.

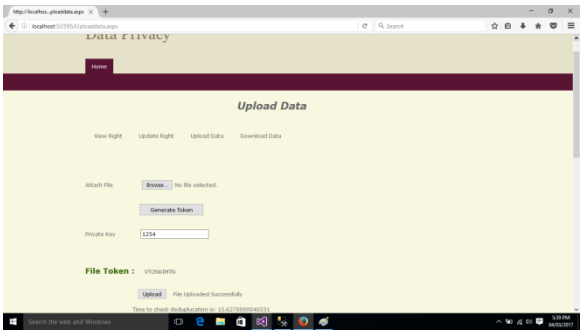


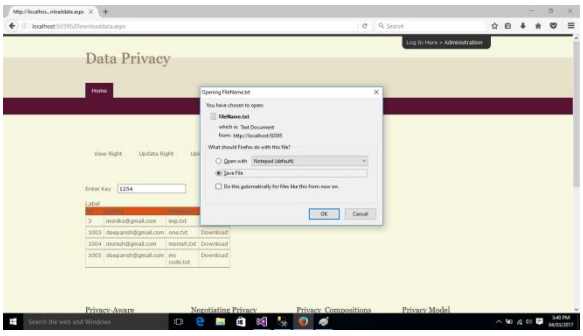
It's a log in page which user is already registered those user login.

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

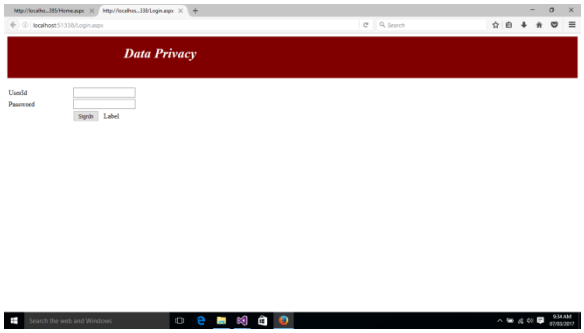




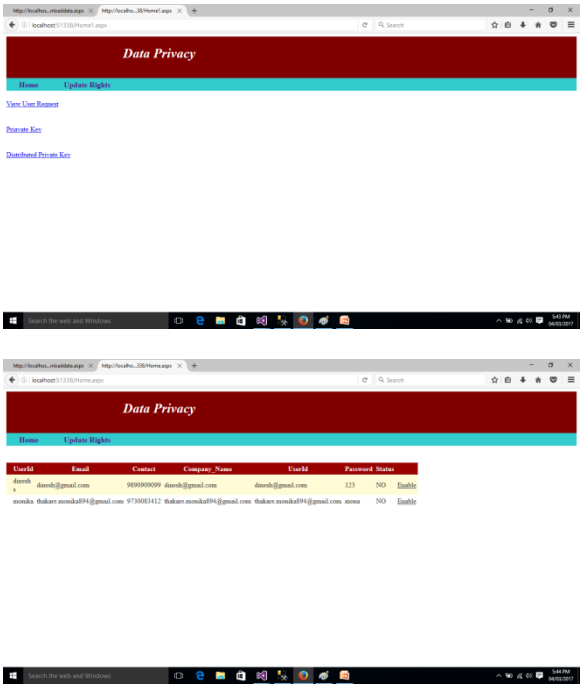




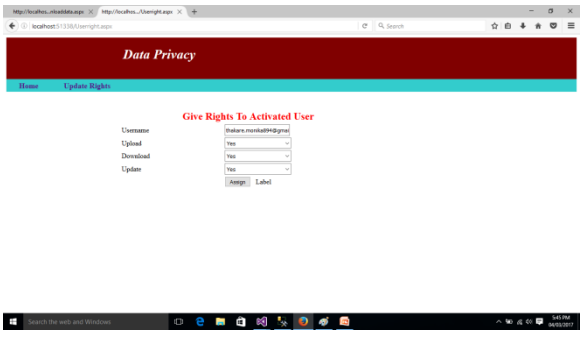
III. Implementation of Proxy server.
This shows admin which having the all rights



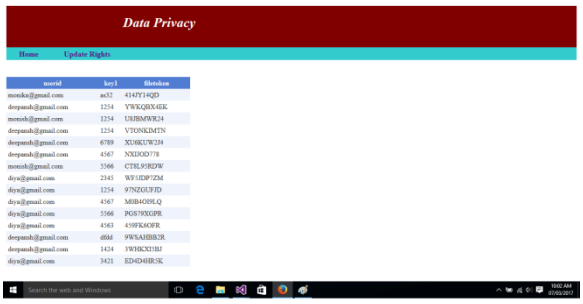
Here shows the all users requests.



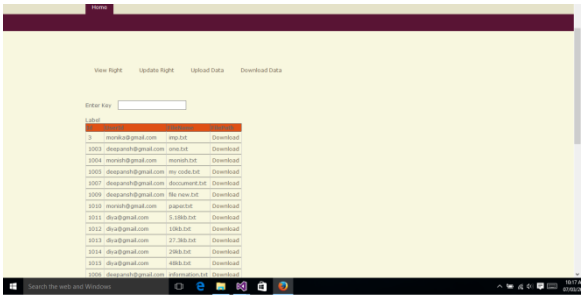
After the user request assign the rights as per user request.



Token will be generated for each file.



Encrypted file can be downloaded from this page.



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.

Proposed System

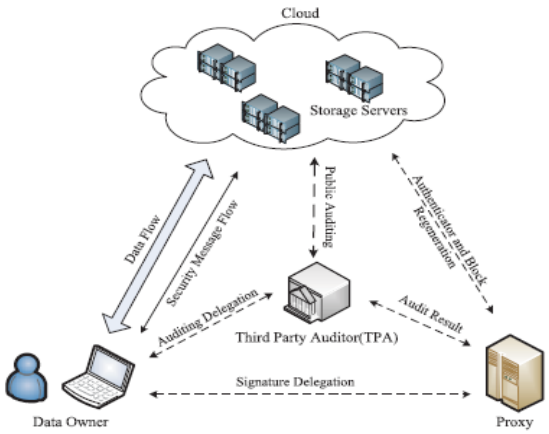


Fig. 1: Cloud Regeneration System Architecture

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.

Comparative Result Analysis

Comparison between existing system and proposed system

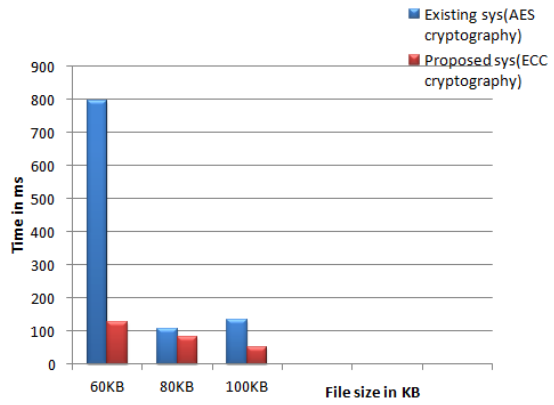


Fig. 2: graph show the comparison of time complexity of files

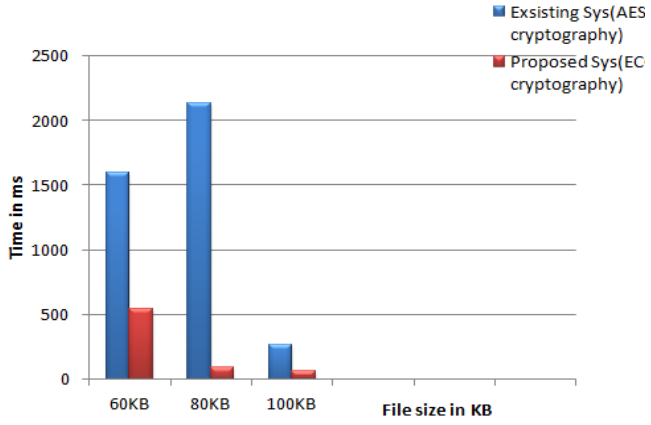


Fig. 3: graph show the computation overhead time of files

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.
20. 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.

21. 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.
22. 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.
23. Dawson, E.; Donovan, D. (1994), "The breadth of Shamir's secretsharing scheme", Computers & Security 13: 69–78
24. Cloud Computing Security: From Singleto Multi-Clouds, 2012, 45th Hawaii International Conference on System Sciences
25. 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.
26. C. Cachin, I. Keidarand A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
27. 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.
28. 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
29. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology. Berlin, Germany: Springer Verlag, 2001, pp. 213–229.
30. 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.
31. 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.
32. 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, 1988.0.