An Efficient Signcryption for Multicopy Dynamic Data Security in Cloud Computing

Pooja Mishra
M.E (CSE) Scholar
Department of CSE,
SIRT-E
Bhopal, India
Pooja.mishra098@gmail.com

Sumit Dhariwal
Asst. Professor
Department of CSE,
SIRT-E
Bhopal, India
Sumitdhariwal22@gmail.com

***Abstract*— Cloud Computing ensures various users to share information or resources over internet. Since the information or data can be shared over internet hence various security issues can be implemented for the prevention this issues. Hence various techniques are implemented for the security of records in public and private clouds. Here a well-organized procedure is implemented based on the concept of signcryption method. The Proposed method implemented here provides security, well as provides load balancing monitoring at the virtual machines and message verification. provides less computational time and data security. The Idea is to create a number of dynamic multiple encrypted copies using Signcryption and then Send these Encrypted Copies over Secure Channel to Cloud Service Provider which is then Stored at multiple Data Centers. The Authorized Users can then Access these Copies from the Data Centers and uses the Decryption key to decrypt the data.**

***Index Terms*— Cloud Storage, Data deduplication, Cloud Computing, Signcryption, Cloud Service Provider, Data Centers.**

I. INTRODUCTION

The fundamental notion of cloud computing is the separation of applications from the operating systems and the hardware on which they run. Cloud computing convey applications via the internet, which are accessible from net browsers and desktop and movable apps, though the software and statistics are stored on servers at an isolated position.

Today, our statistics is wandering yonder the limitations of our individual computers and all our statistics would still safely exist in on the web, available from any Internet-connected computer, anywhere in the ecospheresince of cloud computing.

Cloud makes it possible for operators to usage amenities delivered by haze earners from anywhere at any time. The high development in virtualization and cloud calculating skills imitate the quantity of occupations that are increasing nowadays, necessitate the amenities of the simulated engine. Dissimilar types of occupation preparation processes have been practical on dissimilar types of statistics assignments. Where results are measured with different performance parameters to evaluate the performance.

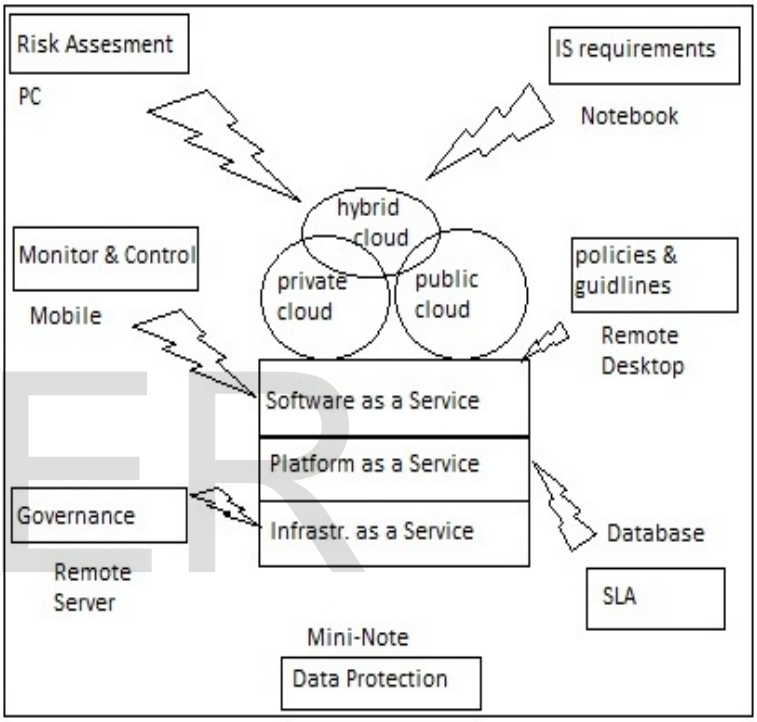

Figure 1: Cloud Computing

Ob-scheduling algorithms are developed to accomplish several areas like probable consequence, effectual use of possessions, low makespan, high quantity, better superiority of package, keeping effectiveness. In job scheduling algorithms, priority of jobs is a challenging issue since some works need to be serviced first than those other jobs which can vacation for an extended period. Appropriate job development procedure must reflect the importance of a job [1]. Figure 1 shows the essential characteristics of cloud computing such as resource combining, wide-ranging system admittance, springiness, on-demand amenities, corporeal cloud capitals(Organization Near) and middleware aptitudes form the root earner of transporting IaaS and PaaS in the form of a collection of transparently data centres and runtime environment and composition tools which comfort the

making, placement and implementation process of application in the cloud. Finally, to provide the above mentioned services, placement replicas such as Community Mist, Secluded Cloud, Cross Cloud and Public Cloud are used by the mist earners. The infrastructure of the cloud is provided publicly to all the general public by the organization in public cloud. Anyone can access services from anywhere publicly. Where, isolated cloud is used for a solitary group only. Previous kind is Mixture Cloud, is a cloud formed by the composition of two or more clouds that is private, community, or public [2].

Cloud Computing is a promising next-generation IT architecture which provides elastic and unlimited resources, including storage, as services to cloud users. It turns out that on one hand sensitive data should be encrypted before uploading to cloud servers. Similar to any untrusted storage case, we can resolve the issue using a cryptographic-based data access control mechanism. We chiefly emphasis on applied request situations such as statistics storing and distribution, as shown by Figure.2, in which proxy attendants are continuously obtainable for providing numerous types of data facilities.

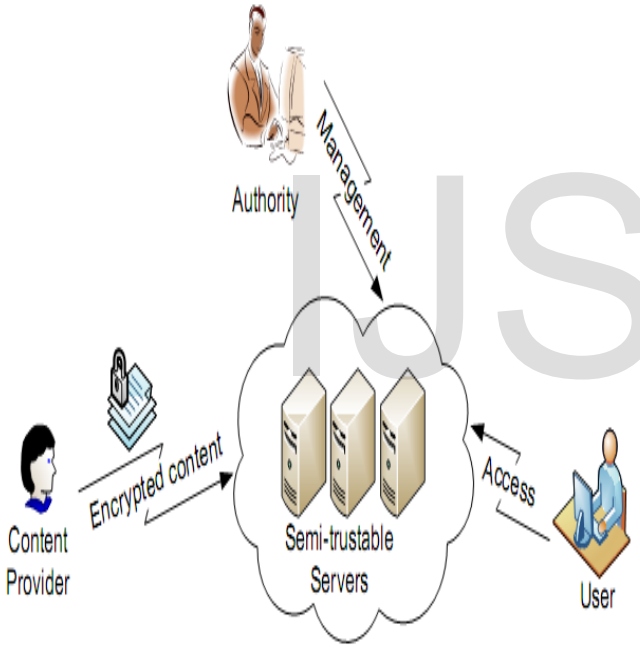

Figure 2: An example application scenario of data sharing.

Similar to previous work [3], these servers are assumed to be curious-but-honest instead of being totally untrusted. In this way our construction places minimal load on the authority upon each revocation event. Existing schemes [4s] suggest associating expiration time attributes to user secret keys. However, the expiration method just enables user revocation at a prearranged time, but is not able to efficiently revoke user attributes on the fly.

Increasingly more and more organizations are opting for outsourcing data to remote cloud service providers (CSPs). Customers can rent the CSPs storage infrastructure to store and retrieve almost unlimited amount of data by paying fees metered in gigabyte/month. For an increased level of scalability, availability, and durability, some customers may want their data to be replicated on multiple servers across multiple data centers. The more copies the CSP is asked to store, the more fees the customers are charged. Therefore, customers need to have a strong guarantee that the CSP is storing all data copies that are agreed upon in the service contract, and all these copies are consistent with the most recent modifications issued by the customers. In this paper, we propose a map-based provable multicopy dynamic data possession (MB-PMDDP) scheme that has the following features: 1) it provides an evidence to the customers that the CSP is not cheating by storing fewer copies; 2) it supports outsourcing of dynamic data, i.e., it supports block-level operations, such as block modification, insertion, deletion, and append; and 3) it allows authorized users to seamlessly access the file copies stored by the CSP. We give a comparative analysis of the proposed MB-PMDDP scheme with a reference model obtained by extending existing provable possession of dynamic single-copy schemes. The theoretical analysis is validated through experimental results on a commercial cloud platform. In addition, we show the security against colluding servers, and discuss how to identify corrupted copies by slightly modifying the proposed scheme [5].

II. Literature Survey

John R. Douceur et. al's provides Reclaiming gap from Duplicate library in a Serverless scattered File structure.[6]. That method is shows that the duplicate-file coalescing system is scalable, highly efficient, and fault-tolerant. The main issue is enabling the identification, and to retrieve planetary from this accompanying replication to type it accessible for skillful file duplication.

In this paper author Jin Li,et.al [7] give explanation for deduplication to save from harm the privacy of susceptible data while sustaining deduplication, the convergent encryption method has been offered to encrypt the data earlier than outsourcing. To improved defend data protection; this paper creates the initial effort to properly concentrate on the difficulty of authorized data deduplication. Different from conventional deduplication methods, the discrepancy benefits of customers are additional well thought-out in duplicate check alongside the data itself. They also present quite a lot of novel deduplication buildings secondary official matching checkered in hybrid cloud construction. As a resistant of notion, they realize a example of our proposed authorized duplicate verify method and accomplish test bed experiments. They show that their proposed authorized duplicate confirm method acquires smallest operating cost evaluated to standard process.

DuPLESS [8] is a real deduplication system, which is built on commercial cloud storage services, that provides security against brute-force attacks launched by malicious clients or an untrusted server. In order to achieve the desired goals while satisfying the required security, an Oblivious Pseudo Random Function (OPRF) protocol and message-locked encryption

(MLE) [9] were utilized for their construction. OPRF is a randomized protocol between clients and the key server, which ensures that the key server learns nothing about the inputs and the resulting outputs, and the clients learn nothing about the key. MLE is a generalized version of convergent encryption designed.

Sharma Bharat et. al's proposed and implemented a Secure and Authorized statistics Deduplication in mixture Cloud with Public audit [10]. Specific clients are only allowable to achieve the matching check and storage provider for distinct files with the equivalent privileges to access. Issue is that duplicate check do not support differential privileges from convergent encryption even though provide confidentiality.

Bhushan Choudhary et. al's provides analysis and Survey of various Data Deduplication Techniques in Cloud [10]. Security by counting differential benefits of clients in the duplicate copy check. Some endangered primitives applied as a part of our harmless de-duplication i.e. Symmetric encryption, Convergent Encryption, Proof of Ownership, Identification Protocol. The security issue is to appraise the effectual operation of cloud band width and disk usage.

Jin Li et. al's proposed and implemented a new advance for protected endorsed Deduplication over Hybrid Cloud Approach [11]. Since Data Deduplication provides eliminating of spare copies of repeating Data and is used to diminish the quantity of storeroom Space. Here in this document duplicate-check token of records are generated by the private obscure Server with Private Keys.

Jorge Blasco et. al's improved Data Deduplication using a Tunable Proof of Ownership using Bloom Filters [12]. Their computational competence in expressions of bandwidth and I/O, for both legal clients and the server. In addition, PoW methods should not entail the server to load the large portion from its back-end storage at each execution of PoW. The main issue is cause root of these risks lies in the precision that proof of ownership only relies on the knowledge of a static, small portion of information.

Wee Keong et. al's also propose a new and efficient technique for the Private Data Deduplication protocol in Cloud Data Storage [13]. It pompous in the framework of two-party computations using private data de-duplication protocol. Algorithm is best for de-duplication protocol for private data storage. How to define the security of private data de-duplication protocols how to formalize the functionality of private data de-duplication protocols, and how to construct private data de-duplication protocols if exist.

N.O. Agrawal et. al's provides a new way of providing Secure Deduplication and Data Security with Efficient and Reliable CEKM [14]. Here in this paper Add security features insider attacker on De-duplication and outsider attacker by using the detection of masquerade activity by risk-averse attackers. The problem of injury of pinched data if we diminution the value of that pinched evidence to the aggressor to achieving effectual and consistent key organization in protected de-duplication

III. Proposed Methodology

1. First of all create a cloud Environment.
2. The cloud Environment Setup consists of 'N' number of Cloudlets, Data Centers, Virtual Machines , Brokers .
3. Now the user of the cloud starts sharing of data to other users of the cloud.
4. During the sharing of data over cloud environment four steps are performed initialized with Setup Phase and Key Generation Phase, Encryption Phase, Decryption and Verification Phase.
5. Here the cloud environment is setup and simulate using Cloud Simulator in which first of all Cloudlets , Data Centers Virtual Machines and Brokers are created.
6. If 'N' be the number of Requests to be send from Cloudlets to the Data Centers through Brokers .
7. Let us suppose number of resources to use during the sharing of data from Cloudlets to Data Centers .
8. For each of the Resource to be shared to data Centers
9. During the setup phase
10. Signcryption methodology implemented here for data security

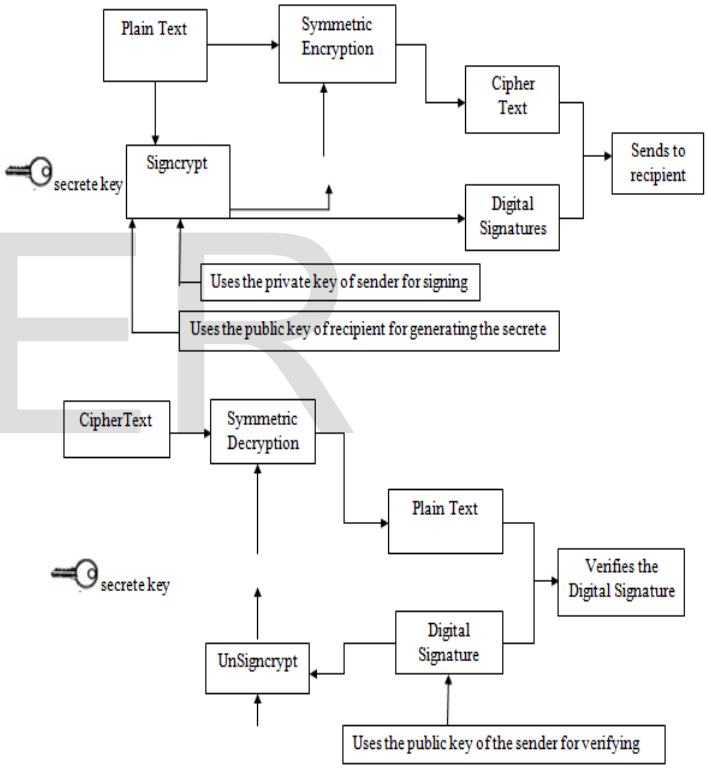

Figure 3. Proposed Methodology

- The signcryption algorithm implemented here uses the Identity of the other users 'ID1'.
- First of all select a random Integer 'r',
- Compute P ← [k] B
- T ← [k] Sk1
- Generate a set of keys from the key Derivation Function (k1||k2) ← KD(T,l)
- Generate Cipher Text using the first Key c ← Ek1(m)

- Generate Signature using the other key using Message Authentication Code
- Sg← MACk2(c).
- Sends the signcrypted text (P, C, Sg) to receiver.

- As soon as the signcrypted message (P, C, Sg)is received to the Receiver with Identity 'IDi'.
- Generate a message String T using T ← [x] P
- Generate a set of Key pairs using Key Derivation Function
- (k1||k2) ← KD(T,l)
- Decrypt the message using Key k1, m ← Dk1(c).
- Generate Signature using the other key using Message Authentication Code
- Sg1← MACk2(m).
- Now verify the message by checking if the generated signatures from the user
- Sg == Sg1
- If equal then message is verified message else invalid.

IV. Result Analysis

The table shown below is the analysis of Proof Computation Time. The analysis is done on number of copies and the proposed methodology has low Proof Computation Time as compared to the Existing Work.

	Proof Computation Time (Sec)	
# of Copies	Existing Work	Proposed Work
1	0.9	0.7
5	1.1	0.8
10	1.2	1
15	1.5	1.3
20	1.8	1.6

Table 1. Analysis of Proof Computation Time

The table shown below is the analysis of Verification Time. The analysis is done on number of copies and the proposed methodology has low Verification as compared to the Existing Work.

	Verification Time (Sec)	
# of Copies	Existing Work	Proposed Work
1	1.6	1.4
5	1.5	1.2
10	1.4	1
5	1.3	0.7
20	1.2	0.6

Table 2. Analysis of Verification Time

The table shown below is the analysis of Owner Computation Time. The analysis is done on number of copies and the proposed methodology has low Owner Computation Time as compared to the Existing Work.

	Owner Computation Time (Sec)	
# of Copies	Existing Work	Proposed Work
1	0.261	0.23
5	1.304	1.15
10	2.608	2.36
15	3.913	3.621
20	5.217	4.84

Table 3. Analysis of Owner Computation Time

The figure shown below is the analysis of Verification Time. The analysis is done on number of copies and the proposed methodology has low Verification as compared to the Existing Work.

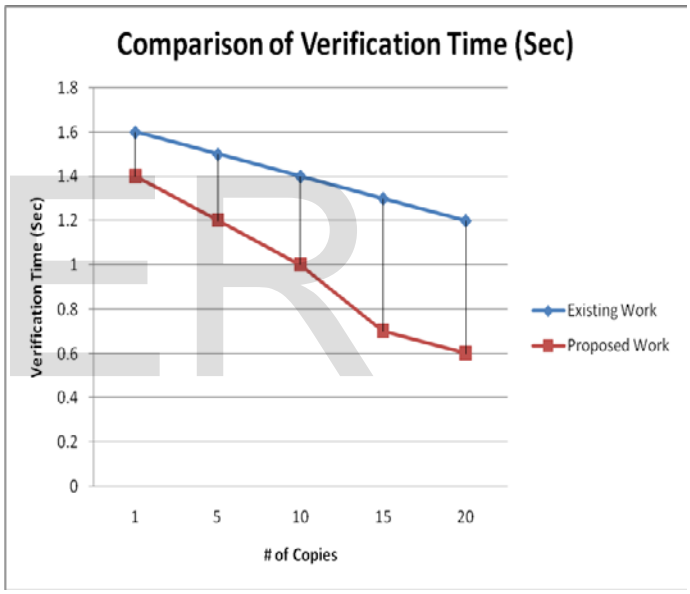

Figure 4. Comparison of Proof Computation Time

The figure shown below is the analysis of Owner Computation Time. The analysis is done on number of copies and the proposed methodology has low Owner Computation Time as compared to the Existing Work.

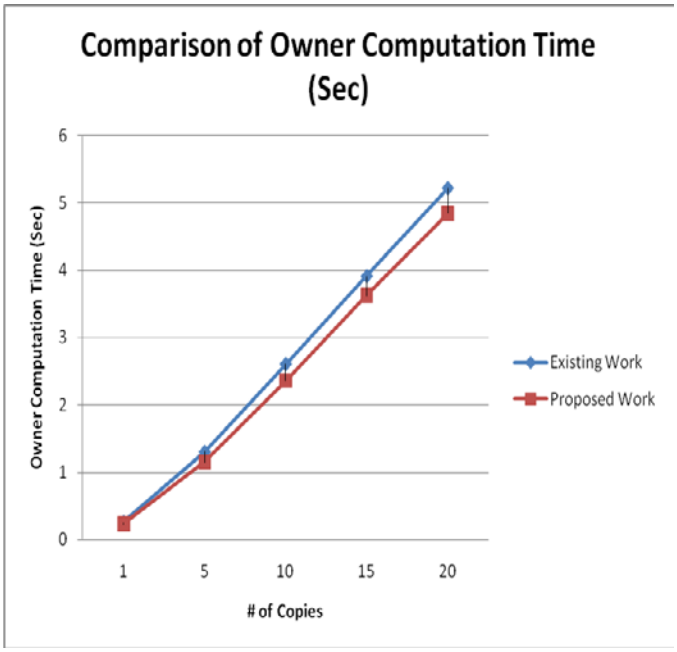

Figure 5. Comparison of Owner Computation Time

The figure shown below is the analysis of Proof Computation Time. The analysis is done on number of copies and the proposed methodology has low Proof Computation Time as compared to the Existing Work.

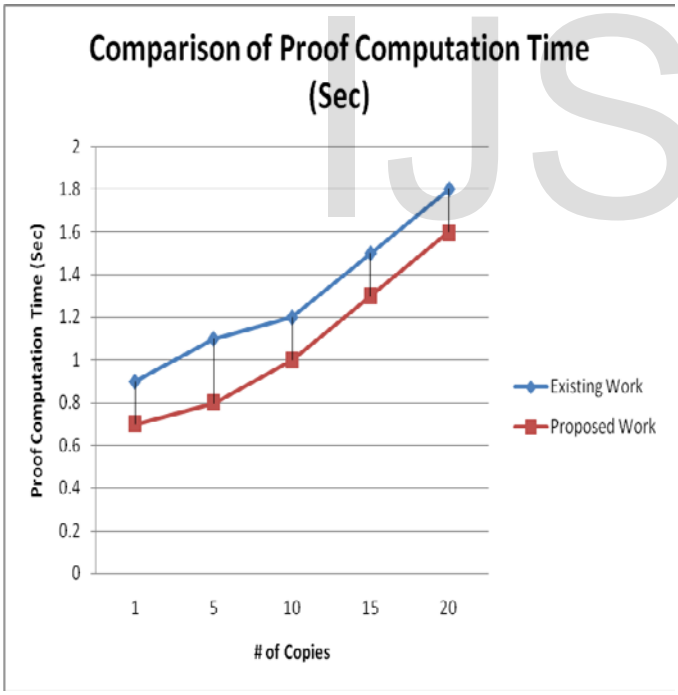

Figure 6. Comparison of Proof Computation Time

V. Conclusion

The proposed methodology implemented here for the efficient data sharing by providing mutual authentication between users of the public clouds. The methodology implemented here provides efficient computational cost and time for encryption and decryption as well as provides secure data communication over public clouds.

The planned methodology implemented here provides efficient results as equated to the existing technique provided for the distributed accountability in cloud computing, but further enhancements can be done for the improvement of the framework and also an effectual system is implemented based on the concept of fuzzy-keyword based key generation.

References

[1] Ghanbari, Shamsollah, and Mohamed Othman. "A Priority based Job Scheduling Algorithm in Cloud Computing." Procedia Engineering 50 (2012): 778-785.

[2] R.Madhubala, "An Illustrative Study on cloud computing", "International Journal of Soft Computing and Engineering", Vol.1, issue.6, January 2012, pp. 286-290.

[3] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. Over-encryption: Management of Access Control Evolution on Outsourced Data. In Proc. of VLDB'07, Vienna, Austria, 2007.

[4] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP'07, Washington, DC, USA, 2007.

[5] Ayad F. Barsoum and M. Anwar Hasan, " Provable Multicopy Dynamic Data Possession in Cloud Computing Systems", IEEE Transactions on Information Forensics and Security, Vol. 10 and No. 3, March 2015.

[6] John R. Douceur, Atul Adya, William J. Bolosky, Dan Simon, Marvin Theimer, "Reclaiming Space from Duplicate Files in a Serverless Distributed File System" July 2002.

[7] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou" A Hybrid Cloud Approach for Secure Authorized Deduplication" IEEE Transactions On Parallel And Distributed System VOL: PP NO:99 YEAR 2013.

[8] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Dupless: Server-aided encryption for deduplicated storage," in Proc. USENIX Security Symposium (SEC'13), pp. 179-194, and 2013.

[9] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," Advances in Cryptology - EUROCRYPT'13, LNCS 7881, pp. 296-312, 2013.

[10] Sharma Bharat, Mandre B.R. "A Secured and Authorized Data Deduplication in Hybrid Cloud with Public Auditing" International Journal of Computer Applications (0975 – 8887) Volume 120 – No.16, June 2015.

[11] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P.C.Lee, Wenjing Lou, " A Hybrid Cloud Approach for Secure Authorized Deduplication", IEEE Transactions on Parallel and Distributed Systems, IEEE 2014.

[12] Jorge Blasco, Agustin Orfila, "A Tunable Proof of Ownership Scheme for Deduplication Using Bloom Filters" June 18, 2014.

[13] Wee Keong Ng, Yonggang Wen, Huafei Zhu, "Private Data De-duplication Protocols in Cloud Storage" ACM 978-1-4503-0857-1/12/03, 2011.

[14] Bhushan Choudhary, Amit Dravid , "A Study on Authorized Deduplication Techniques in Cloud Computing" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 12, April 2014.