ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# PRESERVING IDENTITY OF SHARED DATA STORED IN THE CLOUD USING PUBLIC AUDIT MECHANISM

**Amudhavalli.P *, Dr.A.Chandrasekar**

Research Scholar, Department of Computer Science and Engineering , St.Peter's University, India
Professor, Department of Computer Science and Engineering, St.Joseph's College of Engineering, India

## ABSTRACT

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. The application software and databases are moved to the centralized large data centers, where managing the data and services may not be completely reliable. This work studies the problem of ensuring the integrity and security of data storage in Cloud Computing. We consider a scheme called threshold proxy re-encryption and secure erasure code, to verify the integrity and enhance server-side security of the dynamic data stored in the cloud. In the previous works, ensuring remote data reliability often lacks the support of either public audit ability or dynamic data transactions, this paper achieves both. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from cloud server. In our proposed work we use the multiple servers for storing data to servers. We avoid the additional storage for multi cloud system using split server concept as for security.

**Keyword** : Cloud Computing, Advanced Encryption Standard, Erasure Coding, Distributed System, Check sums, Public Auditing

## INTRODUCTION

The Concept of Cloud Computing has evolved from Cluster, grid and utility computing. Cloud computing is a high-throughput computing paradigm whereby the infrastructure provides the services through a large data center or server farms. The Cloud computing models enables users to share access to resources from anywhere at any time through their connected devices. The cloud offers significant benefit to IT companies by freeing them from the low-level task of setting up the hardware and managing the system software. In this advanced model, user can access and deploy the cloud application from anywhere in the world at very competitive costs. Cloud computing leverages its low cost and simplicity to both providers and users. It intends to leverage multitasking to achieve higher throughput by serving many heterogeneous applications, large or small, simultaneously. In cloud, there are three types of deployment model. They are Private Cloud, Public Cloud and Hybrid Cloud. A

Public cloud is built over the internet and can be accessed by any user who has paid for the service. They are owned by service providers and are accessible through a subscription. A public cloud delivers a selected set of business processes. Some examples of public cloud are Google App Engine, Amazon Web Services, Microsoft Azure, IBM Blue Cloud, etc. A Private Cloud is built within the domain of an intranet owned by a single organization. Therefore it is client owned and managed, and its access is limited to the owning clients and their partners. It gives local users a flexible and agile private infrastructure to run service workloads within their administrative domains. An example of a private .cloud is the one the U.S. National Aeronautics and Space Administration (NASA) are building to enable researchers to run climate models on remote systems it provides. This can save users the capital expense of HPC machines at local sites. A Hybrid cloud is built with both public and private clouds. Private clouds can also support a hybrid cloud model by supplementing local infrastructure with computing capacity from an external public cloud For example, the Research Compute Cloud (RC2) is a private cloud, built by IBM, that interconnects the computing and IT resources at eight IBM Research Centers scattered throughout the United States, Europe, and Asia.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

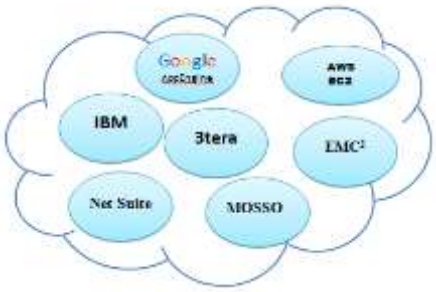



***Fig. 1 Cloud Service Providers***

The Cloud Computing Provides different Service Models. They are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).The SaaS model provides software application as a service. This refers to browser-initiated application software over thousands of cloud customers. Services and tools offered by PaaS are utilized in construction of applications and management of their deployment on resources offered by IaaS providers. The PaaS is able to develop, deploy and manage the execution of applications using provisioned resources demands a cloud platform with the proper software environment. The platform cloud is an integrated computer system consisting of both hardware and software infrastructure. The IaaS model allows users to use virtualized IT resources for computing, storage, and networking. In short, the service is performed by rented cloud infrastructure.


***Fig. 2 Cloud System Models***

There are many advantages in cloud computing, it is pay-as-you-go model, therefore the cost is significantly low because they simply rent computer resources without buying the computer in advance. All hardware and software resources are leased from the cloud provider without capital investment on the part of the users. Only the execution phase costs some money. It improve accessibility and Flexibility, Minimize licensing new software, less personnel training is needed, Streamline process. Apart from this, there is also some obstacles. They are Service Availability and Data Lock-in Problem, Data Privacy and Security concerns, Cloud Scalability, Interoperability and Standardization. Before adopting this technology; the user should know that they will be surrendering all the company's sensitive information to a third-party cloud service provider. This could potentially put their company to a big risk. Hence, the user needs to choose the most trustworthy service provider, who will keep the information totally secure.

The cloud user is responsible for application-level security. The cloud provider is responsible for physical security, and likely, for enforcing external firewall policies. The data which are stored in cloud might be missing or get corrupted due to some hardware/software failure or hacked by a third party which are said to be hackers. The cloud service providers will hesitate to tell the problems of these data errors, since their organization reputation will get affected and also the company's growth gets decreased. Therefore, the integrity of cloud data should be verified before any data utilization, such as search or computation over cloud data. The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures (e.g., RSA) or hash values (e.g., MD5) of the entire data. Recently, many mechanisms have been proposed to do public auditing. In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking [9]. A public verifier could be a data user (e.g.,

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

researcher) who would like to utilize the owner's data via the cloud or a third-party auditor (TPA)[1] who can provide expert integrity checking services. But here we are using the checksum algorithm for checking the integrity of the data and solves the traceability problems.

In This Paper we are using the Secure Erasure Code for Server Side Security. This Algorithm will Split the file into a multiple Server, Encrypt the data using the AES/DES Technique and store the data in the server. Attribute based Encryption is done in this ESS. Also the integrity of the data is achieved by Check Sum Algorithm.

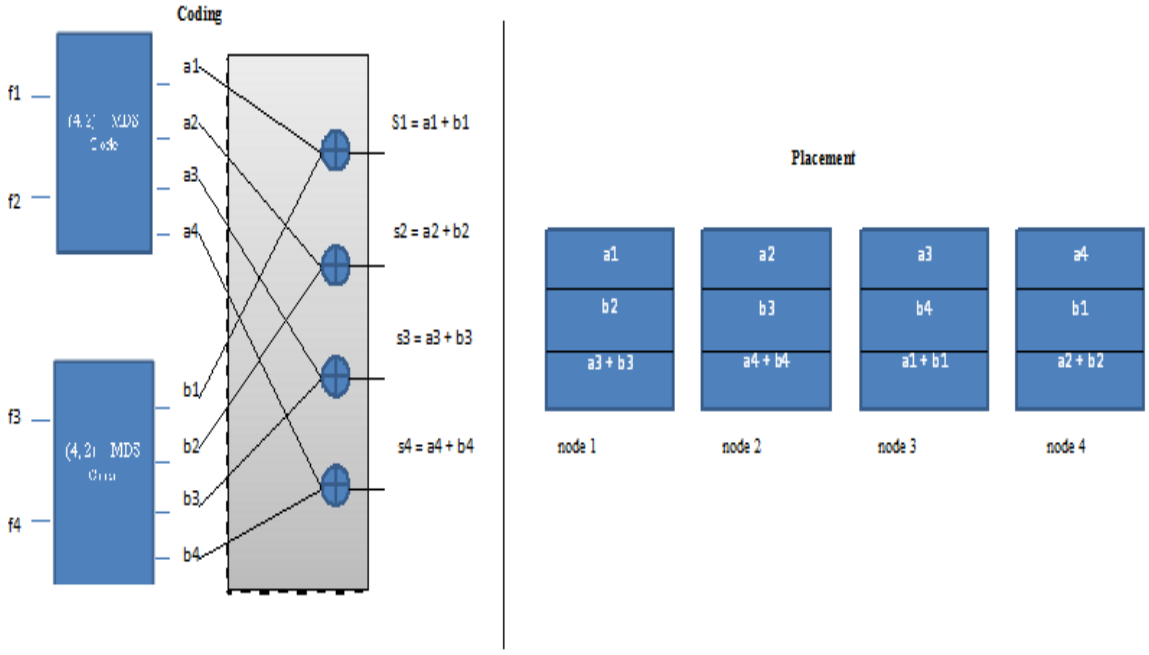
## SYSTEM AND SECURITY MODEL

The main issue is the Security and Integrity/Traceability in the server-side of the existing Cloud environment. To overcome these issues we are proposing Secure Erasure code Algorithm and Check Sum Algorithm respectively.

### *A. Secure Erasure Code Algorithm*

Secure Erasure code [3][10] is an algorithm to encode a message of k symbols into a codeword of n symbols by erasure coding. To store a message, each of its codeword symbols is stored in a different server. A storage server failure corresponds to an erasure error of the codeword symbol. Erasure Coding is a method of Data Protection in which data is broken into Fragments, expanded and encoded with redundant data pieces, and stored across a set of different locations such as disks, storage nodes, or geographic locations. The Distributed Storage system not only supports secure and robust data storage and retrieval but also lets a user forward his data in the storage servers to another user without retrieving the data back.

In this paper, we divide a file into various blocks of size n, after the users have uploaded the file into the server. These each blocks are encrypted using AES (Advanced Encryption Standard) Algorithm. And the encrypted blocks are stored in multiple servers such that no complete file is present in a particular server, (i.e.) files are distributed among the servers. Then in the downloading process the DES Technique is used for Decryption and send back to the user. By doing this, the security in Server-side increases.



ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

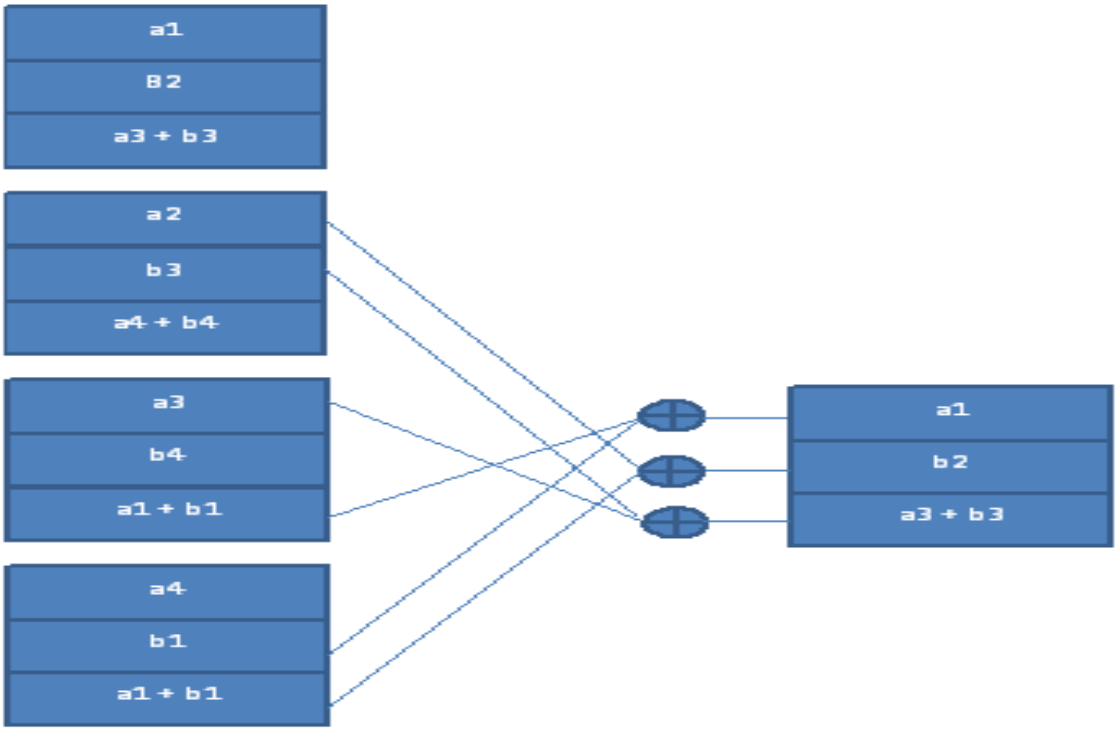



*Fig.3 AES*

### *B. AES-Advanced Encryption Standard Algorithm*

The Algorithm described by AES is a Symmetric Key Algorithm,[6] meaning the same key is used for both Encrypting and Decrypting the data. AES is available in many different Encryption package, and is the first publically accessible and open cipher approved by the National Security Agency (NSA) for top Secret Information when used in a NSA approved in a Cryptographic module.

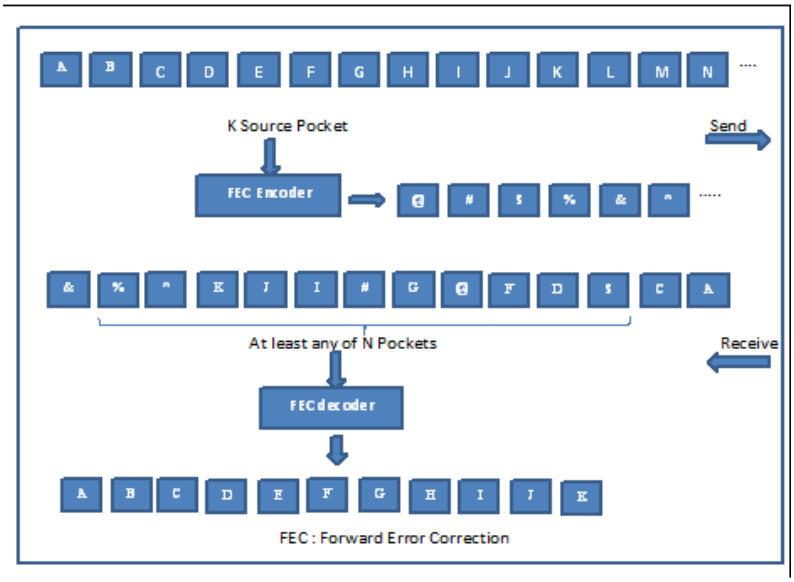



*Fig. 4 Checksum Algorithm*

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

### *C. Checksum Algorithm*

The purposes of data communication, the goal of a checksum[16] algorithm is to balance the effectiveness at detecting errors against the cost of computing the check values. Furthermore, it is expected that a checksum will work in conjunction with other, stronger, data checks such as a CRC. The fact that checksums are typically the secondary level of protection has often led to suggestions that checksums are superfluous.

In this paper, we are proposing that the checksum algorithm can be used for data integrity/traceability while maintaining server side security.

## DESIGN OBJECTIVES

In this paper we introduce five modules to approach secure data storage in Server Side. The five modules are,

- Login and Registration
- Secret key generation
- File uploading process
- Mail alert process
- File Downloading process

### *A. Login and Registration*

A cloud storage system is considered user interface entry level creation in this module. In this Paper we focus on designing a cloud storage system for robustness, confidentiality, and functionality. In this phase, the user will login into a webpage to access his account in the web server. If the user is not registered, then they will register by giving all the necessary details. After login by giving his/her username and password, the webpage will move to a Profile page there will be two options, uploading and downloading options. The User might select the appropriate options for their process.

### *B. Secret Key Generation*

In secret-key cryptography, two or more parties share the same key, which is used to encrypt and decrypt data. The key must be kept secret, and the parties who share a key rely upon each other not to disclose the key and to protect it against modification**.**

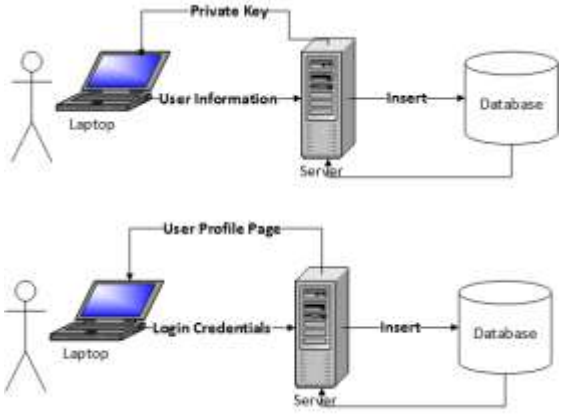



***Fig. 5 Login and Registration***

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

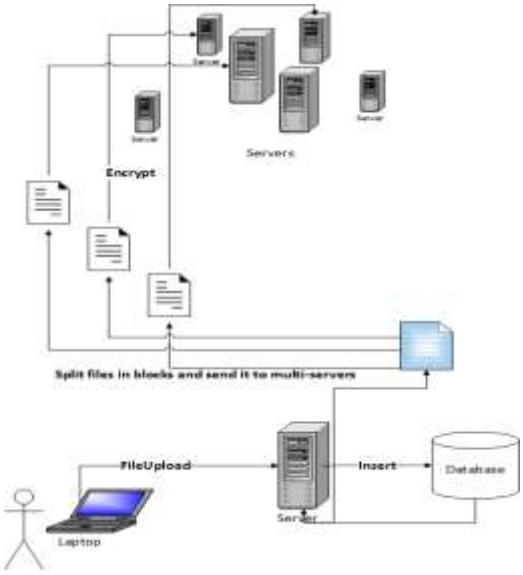



*Fig. 5 File Uploading process*

When the user selects the option file uploading in the Profile page , the server directs to file uploading page. This page consists of a text box and "browse" option for choosing the file for uploading and the file upload option is clicked. After the file is uploaded the file is splited up into various blocks and each block is encrypted using AES algorithm. And each block is stored in multiple servers using "secure erasure algorithm". When this process is taken place successfully a prompt is shown in the user's webpage as "the file is uploaded successfully".

### *C. Mail Alert Process*

When the user wants to retrieve the file which is uploaded by him or shared by his group,the user needs to search or download for the appropriate files.while doing this process the user needs to enter the OTP (One Time Password) which is sent to the users registered mail id or Mobile Phone by the Server.

### *D. File Downloading Process*

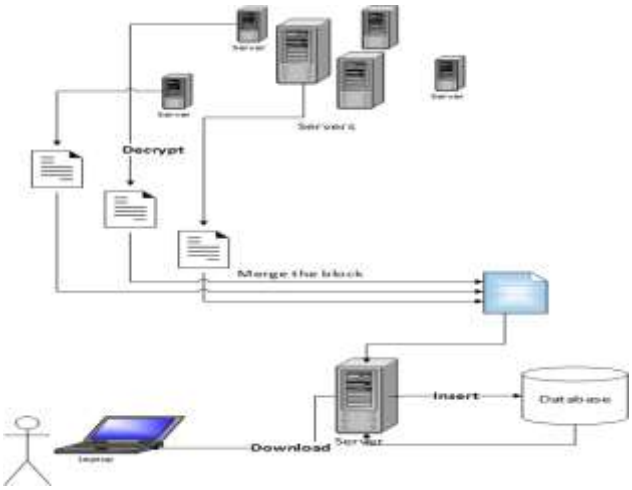



*Fig. File Downloading Process*

File downloading process is the final module in this paper. After searching the file which the user needs he/she might download the file. Once the download button is clicked, the servers containing various blocks of the file is decrypted using

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

a proxy re-encryption technique and is merged together using secure erasure code algorithm. Then, the file is downloaded to user's system.

## RELATED WORKS

We briefly review proxy re-encryption algorithm, de-centralised erasure code, Check- sum algorithm

A proxy server [3] can transfer a cipher text under a private key A to a new one under another public key B. The server does not know the plaintext during transformation. The data is first encrypted with a symmetric data encryption key and then stored in the cloud storage server.

Decentralized erasure codes, [2] which are randomized linear codes with a specific probabilistic structure that leads to optimally sparse generator matrices. These codes can be created by a randomized network protocol where each data node "pre-routes" its data packet to O (log n) randomly and independently selected storage nodes. Each storage node creates a random linear combination of whatever it happens to receive. Therefore each node operates autonomously without any central points of control and with small communication cost.

Checksums use to detect data transmission errors. A checksum [7][16] is an error detection mechanism that is created by "summing up" all the bytes or words in a data word to create a checksum value, often called a Frame Check Sequence (FCS) in networking applications. The checksum is appended to the data word (the message payload) and transmitted with it. Network receivers recomputed the checksum of the received data word and compare it to the received checksum value. If the computed and received checksum match, then it is unlikely that the message suffered a transmission error.

## CONCLUSION

We propose a public auditing mechanism for shared data in the cloud. We utilize check sum algorithm for improving data integrity. Here, we are also using secure erasure code algorithm for preserving server side security.

## REFERENCES

1. Alexandros G. Dimakis, Vinod Prabhakaran, and Kannan Ramchandran "Decentralized Erasure Codes for Distributed Networked Storage", Department of Electrical Engineering and Computer Science, University of California, Berkeley, CA .
2. B. Wang, B. Li and H. Li "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", Proc. IEEE Fifth Intal Conf. Cloud Computing, pp.295 -302 2012
3. Priyadharshini. B.1, Mrs. Carmel Mary Belinda2, M. Ramesh Kumar3," A Secure Code Based Cloud Storage System Using Proxy Re-Encryption Scheme in Cloud Computing", M. E. Student VelTech MultiTech Dr. Rangarajan Dr. Sakunthala Engineering College, Assistant professor VelTech MultiTech Dr. Rangarajan Dr. Sakunthala Engineering College.
4. C.Wang, Q.Wang, K.Ren, and W.Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.
5. K. Ren , C. Wang and Q. Wang "Security Challenges for the Public Cloud", IEEE Internet Computing, vol. 16, no. 1, pp.69 -73 2012.
6. V. Goyal, O. Pandey, A. Saha2i, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in Proc.
7. Theresa C. Maxino, "The Effectiveness of Checksums for Embedded Networks", Department of Electrical and Computer Engineering,Carnegie Mellon University,Pittsburgh, Pennsylvania, USA
8. Q. Zheng and S. Xu, "Secure and Efficient Proof of Storage with Deduplication," in Proc. ACM Conference on Data and Application Security and Privacy (CODASPY), 2012
9. B. Wang , B. Li and H. Li "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE Trans. Services Computing, 2013
10. Hsiao-YingLin , Department of Computer Science,Nat. Chiao Tung University ,Hsinchu,Taiwan Tzeng, W.-G. "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding"

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

11. Gopalan Sivathanu,Charles P. Wright,and Erez Zadok, "Ensuring Data Integrity in Storage: Techniques and Applications " Stony Brook University
12. Rajinder Sandhu , Dr.Inderveer Chana "Securing Virtual Machine in Cloud Enviroment using OVF and Hashing Function "Conf. on Advances in Electronics, Electrical and Computer Engineering ISBN: 978-981-07-6935-2 doi:10.3850/ 978-981-07-6935-2_05.
13. C. Wang , Q. Wang , K. Ren and W. Lou "Ensuring Data Storage Security in Cloud Computing", Proc. 17th Intâl Workshop Quality of Service (IWQoSâ09), pp.1 -9 2009
14. Securing Data Transfer In The Cloud Through Introducing Identification Packet And UDT -Authentication Option Field: A Characterization.
15. R. L. RivFest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). SpringerVerlag, 2001, pp. 552–565.
16. Jonathan Stone, Stanford University , Michael Greenwald, Stanford University, Craig Partridge, BBN Technologies, Jim Hughes, Network System Corporation " Performance of Checksums and CRC s over real data"
17. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Stroage Systems," in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp. 31–42.