ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Data Allocation for Achieving Perfect Secrecy in Multiple Clouds Using Optimal Coding

Deepa R. Nalage, Prof. Prashant Mane

M. E Student, Department of Computer Engineering, Zeal College of Engineering and Research, Pune, India

Professor, Department of Computer Engineering, Zeal College of Engineering and Research, Pune, India

ABSTRACT: In cloud environment, an enormous amount of data is produced everyday. Many organizations are now migrated to cloud and demand for resource is increasing. Hence the providers are now delivering multi-cloud environment to meet this demand. If multiple providers cooperatively work together the availability of resource can be increased. But still clients are worrying that their data is correctly stored and maintained by providers without intact. Though the providers are provide enough security there are still many security issues happening in cloud. Integrity verification of client data is made by using a technique called Provable Data Possession(PDP). This survey paper provides overview about various Provable Data Possession techniques in cloud..

KEYWORDS: Cloud storage, perfect secrecy, information theoretic security, storage allocation

I. INTRODUCTION

Cloud computing is a trend in the present day scenario with almost all the organizations are entering into it. Cloud computing is the collection of virtualized and scalable resources and provide service based on “pay only for use” strategy. It is a faster profit growth point by providing a comparably low-cost, scalable, position-independent platform for clients‟ data. It is constructed based on open architectures and has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. Such a distributed cloud environment is called Multi-Cloud

CHARACTERISTICS:
On-demand self-service -A consumer can unilaterally provision computing capabilities

1. Broad network access - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms

2. Resource pooling - The provider‟s computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

3. Rapid elasticity - Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

4. Measured service - Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

II. RELATED WORK

In the past more research has been conducted into single clouds than into multi-clouds. Multi–clouds can address the security issues that relate to data integrity, data intrusion, and service availability in multi-clouds. In addition, most of the research has focused on providing secure "cloud storage" such as in DepSky. Therefore, providing a cloud database system, instead of normal cloud storage, is a significant goal in order to run queries and deal with databases; in other words, to profit from a database-as-a-service facility in a cloud computing environment

Rocha and Correia et al.(2010) determine possible attackers for IaaS cloud providers. For example, Grosse et al propose one solution is to prevent any physical access to the servers. However, Rocha and Correia argue that the attackers outlined in their work have remote access and do not need any physical access to the servers. Grosse et al. propose another solution is to monitor all access to the servers in a cloud where the user‟s data is stored. However, Rocha and Correia claim that this mechanism is beneficial for monitoring employee‟s behavior in terms of whether they are following the privacy policy of the company or not, but it is not effective because it detects the problem after it has happened.[1]

First approach proposed the PDP model[4] for ensuring possession of files on untrusted storages without downloading the actual data and provided an RSA-based scheme for a static case. It also includes a public verifiability, with this anyone, not just the owner can challenge the server for data possession. This extends the application areas of PDP protocol by separating the data owners and the users. But this is insecure against replay attacks in dynamic scenarios because of dependencies in index of data blocks. Moreover, they are not fit for multi-cloud storage because there is no homomorphism property in the verification process. To overcome static file storage limits in PDP and to provide dynamic data operations in PDP the Scalable PDP [6] model have been proposed. It is a lightweight PDP scheme based on cryptographic hash function and symmetric key encryption. But due to the lack of randomness in the challenges and by using previous metadata, the servers can deceive the owners.

The another drawback in this model is block size and its length are fixed and hence the modification of blocks cannot be done anywhere. Based on this work two Dynamic PDP[7] has been proposed. First is basic scheme, called DPDP-I and Second is the „blockless‟ scheme, called DPDPII. But these schemes are also not effective for a multi-cloud environment .

Second approach is POR scheme[5], it describes the preprocessing steps that the clients should do before sending their file to a CSP. But this also not allow for updating the data efficiently. An improved version of this protocol called Compact POR[8] has been proposed. This technique which uses homomorphic property to aggregate a proof into authenticator value but their solution is also static and could not prevent the leakage of data blocks in the verification process. The dynamic scheme with cost by integrating the Compact POR scheme and Merkle Hash Tree (MHT) into the DPDP has been proposed. Several POR schemes and models have been recently proposed by using RAID techniques. It introduced a distributed cryptographic system that allows a set of servers to solve the PDP problem. It is based on an integrity protected error correcting code (IP-ECC), which improves the security and efficiency of existing tools. Here , a file must be transformed into distinct segments with the same length, which are distributed across servers. It is more suitable for RAID rather than a cloud storage.

III. EXISTING SYSTEM APPROACH

In that system Cloud is Single which at created time cloud are not accessible and cost are very high. mainly In cloud is single means if at certain time cloud are no accessible. This paper is the first one which considers the problem as a whole and derives a jointly optimal coding and storage allocation scheme, which achieves perfect secrecy with minimum cost.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Disadvantages:-

1.Data Integrity.

2.Security are less.

3.Single cloud are not accessible at that time Data are loss.

4.Data losses condition.

IV. PROPOSED SYSTEM ARCHITECTURE

In this proposed system Shamir's secret sharing algorithm is extremely effective for storing the client data securely. It provides authentication to clients and also provide security by encryption and decryption using secret key. Our proposed system can be enhanced by providing effective security by using stronger encryption algorithm. It also provides fast service to store data on server. It also giving proof of integrity of the data to client. This scheme reduce storage overhead of the customer by compressing the data and reduce computational overhead of the cloud storage server.

ADVANTAGES OF PROPOSED SYSTEM

1. Data Integrity
2. Service Availability.
3. The user runs custom application using the service provider's resources
4. Cloud service providers should ensure the security of their customers‟ data and should be responsible if any security risk affects their customers‟ service infrastructure

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

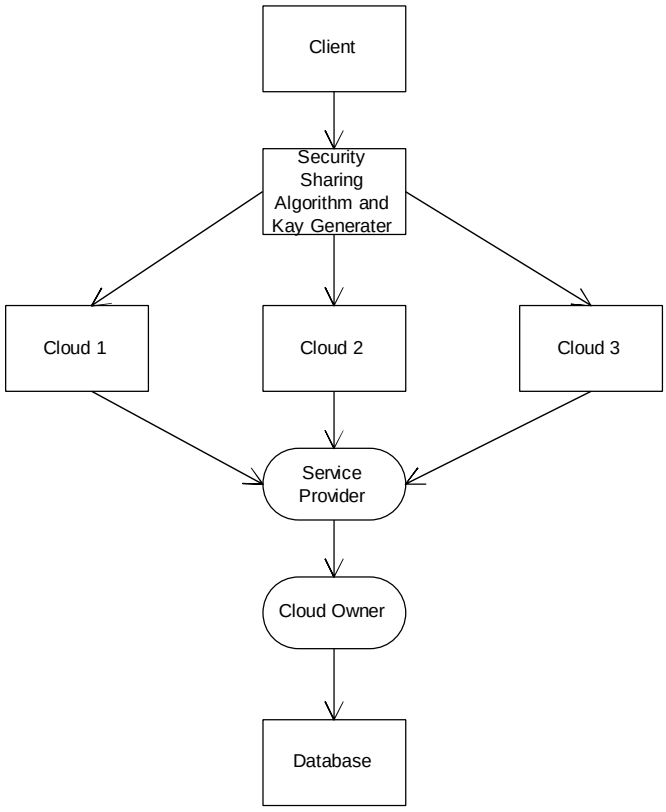


Fig 1.Proposed System Architecture

IV. EXPERIEMNTAL RESULT

In this section, we give some numerical examples on the allocation parameters. In the following examples, we assume that the file size is not large, so the whole file is regarded as a single chuck, which consists of B blocks of data. For a large file, it will be divided into smaller chucks first, and the encoding operations are applied to each chuck repeatedly. For each chunk, we determine the amount of encoded data to be stored in each CSP according to Section VII-A. After that, the code length is determined and the chunk can be encoded according to the method in Section VII-B. The encoded data for a CSP, commonly called a share, can then be stored in the CSPs.

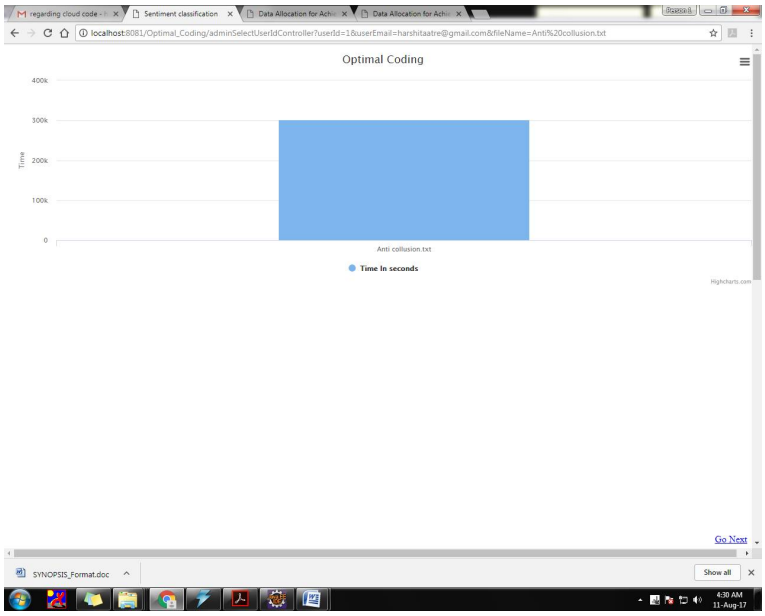
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

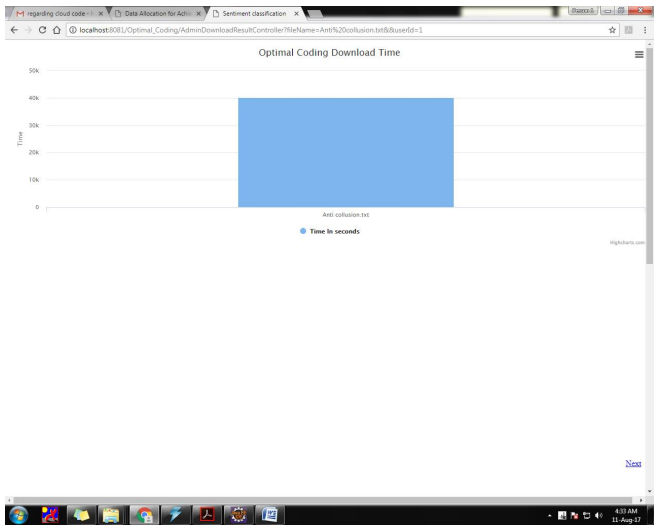
(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017



1. Uploading Time



2. Downloading Time

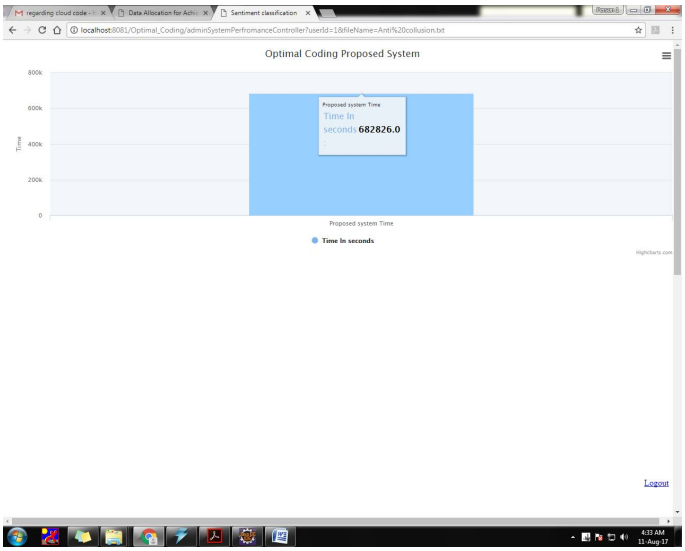
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017



3. Proposed System

V. CONCLUSION

In this paper, we research the minimization of capacity taken a toll when the client stores its information in different untrustful what's more, temperamental mists. We give a lower bound on the expense what's more, present a coding plan that can accomplish this bound. This ideal plan can be comprehended through two-dimensional seek, which has low computational multifaceted nature. Since the computational multifaceted nature is low, the outcome is additionally relevant to extensive scale stockpiling frameworks.

REFERENCES

[1] Ping Hu, Chi Wan Sung "Optimal Coding and Allocation for Perfect Secrecy in Multiple Clouds" IEEE Transactions On Information Forensics And Security, Vol. 11, No. 2, February 2016
[2] M. Armbrustet al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.
[3] Mazhar Ali, Athanasios V. Vasilakos,"SeDaSC: Secure Data Sharing in Clouds", Fellow IEEE Syst. J.,to be published, doi:10.1109/JSYST.2014.2379646.
[4] NeginGolrezaei, Alexandros G. Dimakis, Andreas F. Molisch," Wireless Device-to-Device Communications with Distributed Caching", 2012 IEEE.
[5] Prof.V.N.Dhawas,PranaliJuikar,NehaPatekar,NehaLendghar,SushantVartak," A Secured Cost Effective Multi-Cloud Storage in Cloud Computing", Volume 4, Issue 5, May-2013.
[6] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.
[7] Ms.V.Mangaiyarkkarasiand Mr.K.A.Dhamodaran," A Comparative Survey on Availability and Integrity Verification in Multi-Cloud", Volume 1, Issue 10, December 2012.
[8] Monica G. Charate1, Dr. Savita R. Bhosale," Cloud Computing Security Using Shamir's Secret Sharing Algorithm From Single Cloud To Multi Cloud", Volume No 03, Special Issue No. 01, April 2015.
[9]AngLi,Xiaowei Yang ,"CloudCmp: Comparing Public Cloud Providers", November 1–3, 2010, Melbourne, Australia.
[10] Marten van Dijk, Ari Juels ," On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing", RSA Laboratories.
[11] AdlaShekhar, JanapatiVenkata Krishna," Secure and Reliable Cloud Security from Single to Multi Clouds", volume 16 number 2 – Oct 2014.