ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 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: For a client to store information in the cloud, utilizing administrations gave by different distributed storage suppliers is a promising way to deal with increment the level of information accessibility furthermore, classification, as it is impossible that diverse CSPs are out of administration in the meantime or plot with each other to concentrate data of a client. This paper researches the issue of putting away information dependably and safely in different CSPs

Obliged by given spending plans with least cost. Past works, with varieties in issue definitions, commonly handle the issue by decoupling it into sub-issues and explain them independently. While such a decoupling methodology is straightforward, the resultant arrangement is problematic. This paper is the first which considers the issue all in all and determines a together ideal coding and capacity portion plan, which accomplishes great secrecy with least cost. The analytical result uncovers that the optimal coding plan is the nested maximum-distance-separable code and the ideal measure of information to be put away in the CSPs displays a specific structure.

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

I. INTRODUCTION

For a user to store data in the cloud, using services provided by multiple cloud storage providers (CSPs) is a promising approach to increase the level of data availability and confidentiality, as it is unlikely that different CSPs are out of service at the same time or collude with each other to extract information of a user. This paper investigates the problem of storing data reliably and securely in multiple CSPs constrained by given budgets with minimum cost. Previous works, with variations in problem formulations, typically tackle the problem by decoupling it into sub-problems and solve them separately. While such a decoupling approach is simple, the resultant solution is suboptimal. 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. The analytical result reveals that the optimal coding scheme is the nested maximum-distance-separable code and the optimal amount of data to be stored in the CSPs exhibits a certain structure. The exact parameters of the code and the exact storage amount to each CSP can be determined numerically by simple 2-D search.Now a days the usage of cloud computing is rapidly increased in many companies. For various reasons the small and medium companies are using cloud computing, to access their applications the services are fast and it also reduce their arrangement costs. Cloud service providers should indicate secrecy and safety issues as a matter of high and quick priority. Handling with “single cloud” service providers is becoming less popular with consumers due to potential harms such as service accessibility failure and the chance that there are misusing insiders in the single cloud. In this year, there has been a move in the direction of “multiclouds”, “intercloud” or “cloud-of-clouds”. This paper emphases on the matters related to the data safety context of cloud computing. As data and info will be provided with a third party, cloud computing users want to avoid a not trusted cloud service provider. Guarding private and important info, such as credit card particulars or a patient’s medical records from enemies or misusing insiders is of serious importance. In the addition of, the potential for movement from a single cloud to a multicloud atmosphere is studied and investigation related to safety issues in single and multi-clouds in cloud computing area measured.Remainder for this paper is ordered as follows. defines the starting of cloud computing and its modules. In addition of, the current examples of cloud service providers and the profits of using their services. tells safety risks in cloud computing. Examines the new era of cloud computing, i.e., multi-clouds and current

DOI: 10.15680/IJIRCCE.2017. 05032258

solutions to point the safety of cloud computing, as well as probing their restrictions. Current proposals for future work. NIST defines cloud computing as “a model for allowing appropriate, on-demand network access to a shared pool of configurable computing assets (e.g., networks, storage, servers, services and applications) that can be quickly provisioned and released with nominal management strength or service provider interface”. This model consists of five features, three distribution models, and four arrangement models. The five key features of cloud computing are: on-demand self-service, location independent supply pooling, broad complex access, quick elasticity, and measured service.

II. LITERATURE SURVEY

No	Paper Name	Author Name	Proposed System	Referred Point
1.	A View of Cloud Computing	Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz,	In this paper to reduce that confusion by clarifying terms, providing simple figures to quantify comparisons between of cloud and conventional Computing, and identifying the top technical and non-technical obstacles and opportunities of Cloud Computing.	1. In this Paper we have referred the solution On Cloud Computing Storage.
2.	SeDaSC: Secure Data Sharing in Clouds	Mazhar Ali, Athanasios V. Vasilakos	We proposed the SeDaSC methodology, which is a cloud storage security scheme for group data. The proposed methodology provides data confidentiality, secure data sharing without reencryption, access control for malicious insiders, and forward and backward access control.	1. In this paper, we have referred the solution for Methodology proposedsecures the data against insider threats among a groupof users.
3.	Wireless Device-to-Device Communications with Distributed Caching	NeginGolrezaei, Alexandros G. Dimakis, Andreas F. Molisch	we identify the best possible scaling in the number of D2D collaborating links. Surprisingly, a very simple distributed caching policy achieves the	1. In this Paper, we have referred the solution our proposed algorithm has low time complexity, it

			optimal scaling behavior and therefore there is no need to centrally coordinate what each node is caching.	can be applied to systems involving large number of storagenodes. 2. Apart from the multi-cloud storage scenario, our workmay also find applications to other DSSs, such as wireless device-to-devicesystems as the capacitiesof the storage nodes in these systems are different.
4.	A Secured Cost Effective Multi-Cloud Storage in Cloud Computing	Prof.V.N.Dhawas,PranaliJuikar,NehaPatekar,NehaLendghar,SushantVartak	In this paper, we propose a secured cost-effective multi-cloud storage model in cloud computing which holds an economical distribution of data among the available Service Providers in the market, to provide customers with data availability as well as secure storage.	1. In this paper, we have referred the solution our proposed a secured cost-effective multi cloud storage in cloud computing.
5.	Communication theory of secrecy systems	C. E. Shannon	In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography.	1. In this paper, we have referred the solution perfect secrecy.

6.	A Comparative Survey on Availability and Integrity Verification in Multi-Cloud	Ms.V.Mangaiyarkkarasiand Mr.K.A.Dhamodaran	This survey paper provides overview about various Provable Data Possession techniques in cloud..	1. In this Paper, we have referred the solution of variousavailability and integrity verification schemes and itsmethodology are classified along with their adaptation tosingle/multi cloud environment.
7.	Cloud Computing Security Using Shamir's Secret Sharing Algorithm From Single Cloud To Multi Cloud	Monica G. Charate1, Dr. Savita R. Bhosale	This paper is carried out to design single and multi-cloud using secret key sharing algorithm which will result in deduction of the cost for the physical infrastructure, reducing the cost entry and execution as well as the response time for various associated applications.	1. In this paper, we have referred the solution for performance of the Shamir's secret sharing scheme, is used in a multicloud environment.
8.	CloudCmp: Comparing Public Cloud Providers	AngLi,Xiaowei Yang	In this paper, this work presents the first tool, CloudCmp, to systematically compare the performance and cost of cloud providers along dimensions that matter to customers.	1. In this Paper, we have referred the solution for the best-performing provider for their applications.
9.	On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing	Marten van Dijk, Ari Juels	Cryptography is an oft-touted remedy. Among its most powerful primitives is fully homomorphic encryption (FHE), dubbed by some the	1. In this Paper , we have referred the solution formally define a hierarchy of natural

			field's and recently realized as a fully functional construct with seeming promise for cloud privacy.	classesof private cloud applications, and show that no cryptographic protocolcan implement those classes where data is shared among clients.
10.	Secure and Reliable Cloud Security from Single to Multi Clouds	AdlaShekhar, JanapatiVenkata Krishna	This paper studies recent investigation related to single and multi-cloud security and addresses . It is found that the investigation into the use of multi-cloud service providers to keep security has received less attention from the study community than has the use of single clouds. This effort aims to help the use of multiclouds due to its capability to reduce security threats that move the cloud computing user.	1. In this Paper, we have referred the solution We have to support migration to multi-clouds due to itsskills to reduce safety risks that affect the cloud computinguse r.

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.

Disadvantages:-

1.Data Integrity.
2.Security are less.
3.Single cloud are not accessible at that time Data are loss.
4.Data losses condition.

DOI: 10.15680/IJIRCCE.2017. 05032258

IV. PROPOSED SYSTEM APPROACH

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:-

1. Data Integrity
2. Service Availability.
3. The user runs custom applications 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

V. SYSTEM ARCHITECTURE

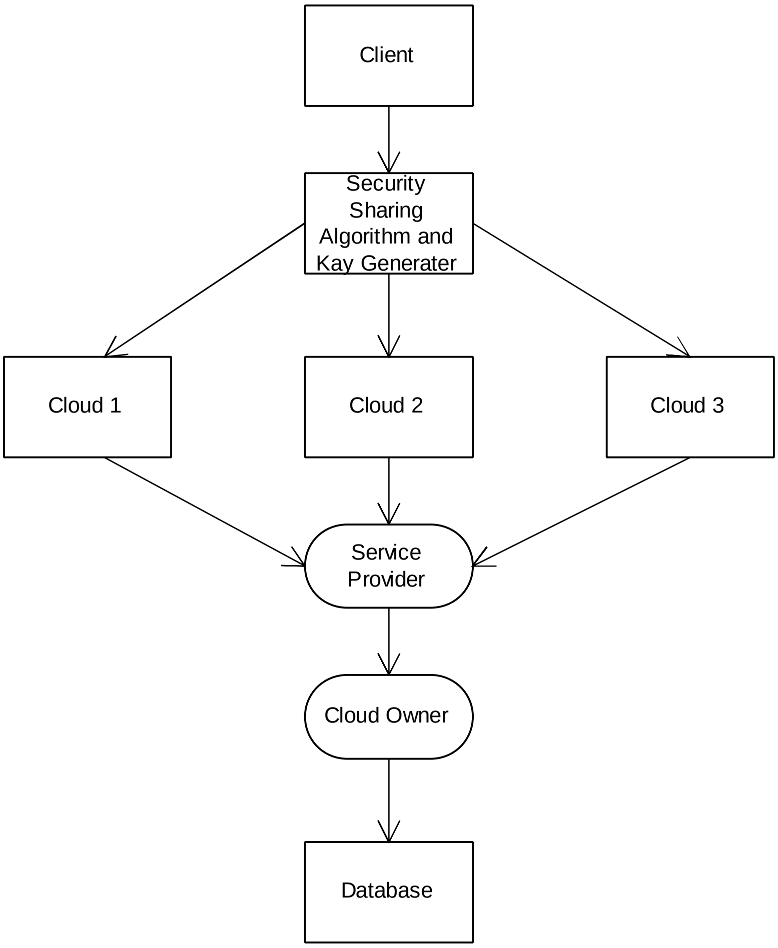

Fig No 01 System Architecture

DOI: 10.15680/IJIRCCE.2017. 05032258

VI. ALGORITHM USED

1. Fragment Algorithm

Considering the existing massive volumes of data processed nowadays and the distributed nature of many organizations, there is no doubt how vital the need is for distributed database systems. In such systems, the response time to a transaction or a query is highly affected by the distribution design of the database system, particularly its methods for fragmentation, replication, and allocation data **fragmentation** is a phenomenon in which storage space is used inefficiently, reducing capacity or performance and often both.

Algorithm for fragmentation:

```
1.  file is to be split go to step 2
2.  Input source path, destination path, Source File, no.of fragments
3. Nof= no.of fragments
3.  Size= size of source file
4. Fragments=size/Nof
10.End
```

Purpose :Splits the file into number of block.

2. RSA Algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it.

1. Choose p = 3 and q = 11
2. Compute n = p * q = 3 * 11 = 33
3. Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
4. Choose e such that 1 < e <φ(n) and e and n are coprime. Let e = 7
5. Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
6. Public key is (e, n) => (7, 33)
7. Private key is (d, n) => (3, 33)
8. The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
9. The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

3. Secret sharing Algorithm

- Goal is to divide some data *D* (e.g., the safe combination) into n pieces D1,D2….Dn in such a way that:
  - Knowledge of any k or more D pieces makes D easily computable.
  - Knowledge of any k -1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).
- This scheme is called (k,n) threshold scheme. If k=n then all participants are required together to reconstruct the secret.
- Choose at random (k-1) coefficients a1,a2,a3…ak-1 , and let S be the a0
- Suppose we want to use (k,n) threshold scheme to share our secret S where k < n.
- Construct n points (i,f(i)) where i=1,2…..n
- Given any subset of k of these pairs, we can find the coefficients of the polynomial by interpolation, and then evaluate a0=S , which is the secret.

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Example:

- Let S=1234
- n=6 and k=3 and obtain random integers a1=166 and a2=94
- Secret share points (1,1494),(2,1942)(3,2598)(4,3402)(5,4414)(6,5614)
- We give each participant a different single point (both x and f(x)).

VII. PERFORMANCES MEASUREMENT

1: Confidentiality - Outsourced information has to be protected from users which are not allowed access, the CSP.
2: Integrity - Outsourced data must keep undamaged on cloud servers. Authorized users and the information owner should be empowered to recognize information corruption.
3: Access control – Authorized users only have to be permitted to gain access to the information that was outsourced.
4: The defense of CSP - The CSP has to be safeguarded against fake accusations that could be stated by owner/users that were dishonest, and this type of malicious conduct is needed to be disclosed.

VIII. MATHEMATICAL MODEL

$X=(x_1,x_2,x_3,x_4.....................x_B)$
Here B block of data

$H(x)=B \log_2 q$ bits.
Let *N* be the number of available CSPs for the user to store data. Before storing the file, the user encodes the *B* blocks of data into *n* blocks. We use

$f: F^B = F^n$

which maps ***x*** into ***y***, to denote the *encoding function*

$y=(y_1,y_2,y_3,\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots y_n)$

for i=1,2,3…………………………N

here N is sub-vectors

let $y_i=(y_{i,1},y_{i,2},\ldots\ldots\ldots..y_{i,ni})$ € F^{ni}

Be the data stored on CSP(Cloud Services provider)

$$n=\sum_{i=1}^{N} n_I \qquad (1)$$

n= total number of encoded block
$\sum_{i=1}^{N} n_I$ =sum of Number of Encoded block stored in each CSp.

Let,
V_i for i € N be the amount of blocks which can be downloaded from CSP *i* within a predefined time delay, it is required that

$$n_i \leq Vi \qquad (2)$$

In this work we assume *Vi* 's are integers, *Vi* ≥ 1 and distinct for $i \in N$. We call *Vi*the *budget* of the stored data on CSP *i*. Let *Ci*be the cost for storing one block of data on CSP *i* and *Ci*'s are all distinct. The total storage cost is given by

$$C=\sum_{i=1}^{N} C_i n_i \quad (3)$$

$$H(x|y(S)) =0, \forall S \cap_{k\,N} \quad (4)$$

The Above bound on H(x) holds for any $S \cap_k N$ and any T is a subset of S.

Therefore (5) can be re-written as

$$H(x)\leq\log_2 q \min(\sum n_i-\sum n_i) \quad (5)$$

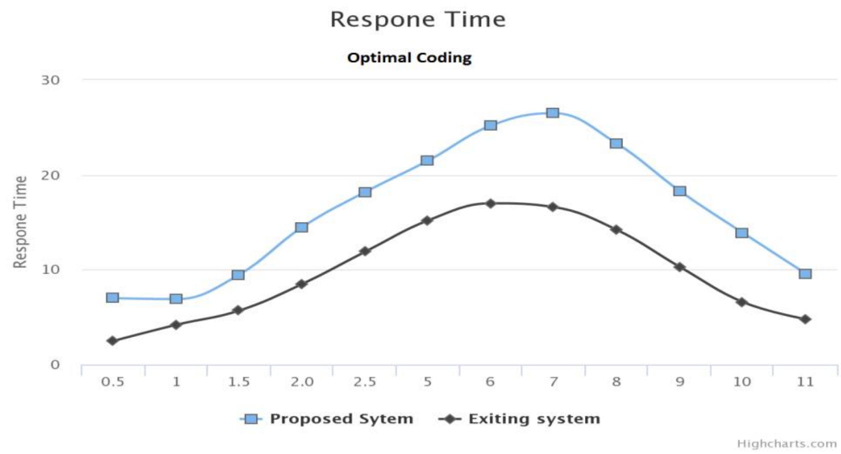

Fig No 02 Comparison of Existing and Proposed System

IX. CONCLUSION

In this paper, we research the minimization of capacity taken a toll when the client stores its information in different untruthful 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.