An Approach Secret Sharing Algorithm to Provide Security to Multi Cloud Data Storage

Ms. Prajakta Kshirsagar[1] Prof. Trupti Gurav[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]SKNCOE, Pune, Savitribai Phule Pune University Maharashtra India

Abstract— Cloud computing is an emerging technology that is at the top in the IT industry. In recent years use of Cloud computing in different mode like cloud storage, cloud hosting, cloud servers are increased in industries and other organization as per requirements. These days rapid use of cloud computing in several IT industries and organizations offers new software at a reasonable cost. Data is used, processed and stored in cloud environment all over the world. With, this there is unlimited benefits but by considering the power, stability and the security of cloud one can't ignore different threats, security risks to user's data on cloud storage. So it is not very promising to depend on a single service provider for outsourced data. However, single cloud providers are less popular among customers because of service unavailability and malicious insiders that exists in single cloud. In proposed system we are implementing the concept of multi-cloud storage where rather storing complete file on single cloud system will split the file in different chunks after encrypt and store it on different cloud. It is one of the main hurdle to share sensitive data with cloud storage providers. For securing outsourced data encryption and secret sharing algorithms are the techniques used extensively to secure outsourcing data. Managing CIA (Confidentiality, Integrity, and Availability) is a main issue and due to this issues, users are opting for multi-cloud as these are secured with various techniques and one of these techniques is secret sharing algorithms. The paper applies Shamir's Secret Sharing Algorithm which will address possible methodologies and solutions to secure outsourcing data in multi clouds. The main focus of this paper will be on data security and provide integrity.

Key words: Data Security, Integrity, Multi-Cloud, Shamir's Secret Sharing Algorithm, Storage

I. INTRODUCTION

Cloud computing is a model for enabling convenient on demand network access to shared recourses. So, can say cloud computing is a technology that is highly scalable, flexible and offers service on demand delivery platform to provide business over the internet. The resources of cloud computing can be extracted fast and in an effortless way which can be scaled with diverse procedures, applications and services that are supplied on demand service in spite of the results that happen because of user location or device. It deliver various services such as software, hardware, data storage, infrastructure over internet. User can access this services through application via internet. Thus, through cloud computing organizations can improve their service deliverance efficiencies. An important thing is that cloud service providers should give urgent priority to security. Handling with "single cloud" service providers is becoming less popular with consumers due to possibility of service failure and the chances that there are misusing insiders in the single cloud. In this era, there has been a movement in the direction of "multi clouds" or "cloud of clouds".

For a user to store data in the cloud, using services provided by multiple cloud storage providers (CSPs) it is very challenging to increase the level of data availability and confidentiality. This paper investigates the problem of storing data reliably and securely in multiple CSPs by given budgets with minimum cost. Past works with variations in problem formulations, tackle the problem by decoupling it into subproblems and resolving them separately. Such a decoupling approach is simple, but the resultant solution is suboptimal. To achieve perfect secrecy with minimum cost this paper considers the problem as a whole and derives a jointly optimal coding and storage allocation scheme.

The aim of this paper is data security aspect of cloud computing where data and security will be shared without any hacks with the third party. All the cloud users do not want to rely on cloud providers that can't be trusted for personal and important details like their credit or debit card or medical report from the malicious insiders and hackers is crucial. This will give a secured cloud database to avoid risks. Here we apply multi clouds concept making use of Shamir's Secret algorithm which will minimize the risk of data intrusion and loss of service availability to ensure data.

As the data and information is provided to third party, cloud computing users want to avoid a untrusted cloud service provider. Protecting private and important information, such as credit card particulars or medical records from attackers or misusing insiders is very important. This paper investigate the new era of cloud computing, i.e., multi clouds and security by using secret sharing algorithm. The main focus of this paper will be on data security and reducing security risks.

II. RELATED WORK

In [2] proposed system reduces confusion by clarifying terms by providing simple figures to quantify comparisons between of cloud and conventional Computing and identifies the top technical and non-technical obstacles and opportunities of Cloud Computing. SeDaSC methodology provide security for group data [3]. The proposed methodology provide cloud storage security scheme which provides secure data sharing without re encryption, data confidentiality access control for malicious insiders, and secures data against forward and backward access control.

Proposed system in [4] introduces the D2D architecture and formulate some theoretical problems also identifies the best possible scaling in the number of D2D collaborating links. A very simple caching distributed policy which optimizes the D2D collaboration distance and analyze the scaling behaviour that achieves the optimal scaling

behavior of D2D benefits and therefore there is no need to centrally coordinate what each node is caching.

[5] Proposed approach provides a secured cost effective multi cloud storage decision model in cloud computing which provide security in such a way that, none of the service provider can successfully retrieve meaningful information from the data pieces allocated at their servers also holds an economical distribution of data among the available service providers to provide customers with data availability as well as confidentiality i.e. security of storage. In [6] a theory of secrecy systems is developed. The theoretical approach which is intended to complement the treatment found in standard works on cryptography. Moving from single clouds to multiclouds is reasonable and important for many reasons. Services of single clouds are still subject to outage. In addition, [25] showed that over 80 percent of company management fear security threats and loss of control of data and systems.

[14] assumes that the main purpose of moving to interclouds is to improve what was offered in single clouds by distributing reliability, trust, and security among multiple cloud providers. In addition, reliable distributed storage [15] which utilizes a subset of BFT techniques was suggested by [14] to be used in multi-clouds. A number of recent studies in this area have built protocols for interclouds. RACS (Redundant Array of Cloud Storage) [13] for instance, utilizes RAID-like techniques that are normally used by disks and file systems, but for multiple cloud storage.

[19] assume that to avoid vender lock-in, distributing a users data among multiple clouds is a helpful solution. This replication also decreases the cost of switching providers and offers better fault tolerance. Therefore, the storage load will be spread among several providers as a result of the RACS proxy [13].

Another security mechanism by name HAIL was introduced in [24] in order to improve service availability. This work is done in multicloud environments. HAIL (High Availability and Integrity Layer) [24] is another example of a protocol that controls multiple clouds. HAIL is a distributed cryptographic system that permits a set of servers to ensure that the clients stored data is retrievable and integral. HAIL provides a software layer to address availability and integrity of the stored data in an intercloud[24]. [11] present a design for intercloud storage (ICStore), which is a step closer than RACS and HAIL as a dependable service in multiple clouds. Cachin et al. [25] develop theories and protocols to address the CIRC attributes (confidentiality, integrity, reliability and consistency) of the data stored in clouds.

As mentioned before, [10] present a virtual storage cloud system called DepSky consisting of a combination of different clouds to build a cloud-of-clouds. [10] Discuss some limitations of the HAIL protocol and RACS system when compared with DepSky. HAIL does not guarantee data confidentiality, it needs code execution in their servers, and it does not deal with multiple versions of data. None of these limitations are found in DepSky [10], whereas the RACS system differs from the DepSky system in that it deals with

Economic failures and vendor lock-in and does not address the issue of cloud storage security problems. In addition, it also does not provide any mechanism to ensure data confidentiality or to provide updates of the stored data.

Finally, the DepSky system presents an experimental evaluation with several clouds, which is different from other previous work on multi-clouds [10]. There are a number of studies on gaining constancy from untrusted clouds. For instance, similar to DepSky, Depot is the security mechanism proposed in [22] in single cloud context. Depot improves the flexibility of cloud storage believe that cloud storages face many risks [22].

However, Depot provides a solution that is cheaper due to using single clouds, but it does not tolerate losses of data and its service availability depends on cloud availability [10]. Other work which implements services on top of untrusted clouds are studies such as SPORC [20] and Another security mechanism by name Venus is used in [23] for data integrity in the single cloud context. Venus [23]. These studies are different from the DepSky system because they consider a single cloud (not a cloud-of-clouds).

In addition, they need code execution in their servers. Furthermore, they offer limited support for the unavailability of cloud services in contrast to DepSky [10].

III. ARCHITECTURE

Till 2010, eighty percent research was carried on single clouds whereas only 20 percent was done in multi clouds.

There are some issues related to single Cloud model

- Data Integrity loss.
- Less Security.
- Single cloud are not accessible at that time Data are loss.
- Data intrusion problem.

To overcome above mentioned issues in existing system we need multi cloud model. Many cloud service provider give storage as a service. They take the data from the user and stored on the large data centers, hence providing a storage. Although due to less security there have been some cases where data is been modified or lost.

In Multi Cloud environment services are improved by distributing reliability, trust and security among various cloud providers. This paper considers the entire problem and make out a jointly optimal coding and storage allocation scheme, which achieves perfect secrecy with minimum cost.

IV. PROPOSED SYSTEM MECHANISM

In proposed system we are implementing the concept of multiple cloud storage with enhanced security using encryption and splitting techniques. In proposed system we need a careful economical distribution of data among the available service provider to provide customer data availability as well as confidentiality using Shamir's secret sharing algorithm which is extremely effective for storing the client data securely. The approach will provide a model to cloud computing users, in order to provide a better security in such a way that, none of the service provider can successfully fetch meaningful information from the data pieces allocated at their servers. In proposed system security can be enhanced by providing effective stronger encryption algorithm. Also, provides fast service to store data on server, gives 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.

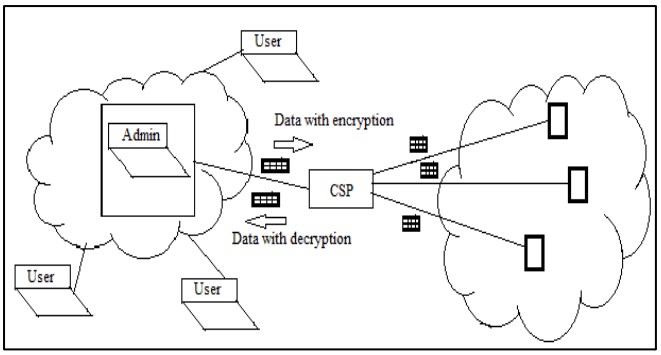

Fig. 1: System Architecture

A. Advantages

- Data Integrity
- Service Availability.
- The user run custom applications using the service provider's resources.

Cloud service providers should assure the security of their customers data and should be responsible if any security risk affects their customers service infrastructure.

V. ALGORITHMS USED

A. Shamir Secret Key Sharing Algorithm

Data can be lost or compromised in the cloud. Therefore, it is important to keep the data secured in the cloud environment. For this, to secure the data in multi-cloud, Shamir proposed to store the data in more than one cloud and encrypt the same in the cloud before it is transferred and saved. 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 the parts are needed to reconstruct the secret. Counting on all participants to combine the secret might be impractical therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

1) Mathematical Definition

The aim of the algorithm is to divide the data in n pieces (DATA1, DATA2, DATA3, DATA4 ….. DATAn) so that,

- Retrieving any k or more DATA pieces will make DATA easily computable.
- Retrieving any k-1 or fewer DATA pieces will leave the DATA completely undetermined.

The above scheme is known as threshold (k, n). If k=n, then all the pieces are there for construction of DATA again. The purpose of Shamir's secret sharing algorithm is that k points are enough to define a polynomial of degree k-1. Example, 2 points are enough to define a line.

Select an approximate k-1 coefficients c0 , c1 , c2 , c3...c(k-1) in H, and let c0 = S, where S is the Secret data which will be stored in cloud.Build the polynomial,

$$H(z) = c0 + c1z1 + c2z2 + \ldots + c(k-1)z(k-1).$$

Then n points are defined, for example set i=1,2…n to retrieve (i, H(i)). A pair is formed with the input to the polynomial and output. Given any subset of k of these pairs, using the interpolation the coefficients of the polynomial which can be found and the constant term a0 is the secret.

2) Shamir's Algorithm Approach

The secret is now divided into pieces by keeping into consideration the approximate degree polynomial which **is**

$$H(z) = c0 + c1z1 + c2z2 + \ldots + c(k-1)z(k-1)$$

In this, c0 = S, S1 = H(1), S2 = H(2),…, Sn = H(n) and represent every share as a point (zi , G(zi) = yi)

3) Example

The example stated below provides the algorithm. To understand, the integer arithmetic is used in place of a scientific based arithmetic or any other vector. Thus, the example illustrated does not ensure perfect secrecy and is therefore not a perfect example of Shamir's scheme.

4) Encryption & Preparation

- Take 1999 as the secret data.
- Dividing it in6 parts (n = 6).
- Parts that are needed to reconstruct the secret is 3 parts (k = 3).
- 2 numbers are selected at random.
- Let them be 154 and 19. c1 = 154 and c2 = 19.
- Our polynomial to produce shares:
- H(z) = 1999 + 154z + 19z2
- 6 parts are made from the polynomial.
- (1, 2172); (2, 2383) ; (3, 2632) ; (4, 2919) ; (5, 3244) ; (6, 3607)
- The diverse single point is given to each participant, both z and H(z).

5) Reconstruction

Any 3 points are enough to reconstruct the secret. Assume: (a0, b0): (2, 2383): (a1, b1): (4, 2919); (a2, b2): (5, 3244)

Now Lagrange basis polynomials will be applied:

- l0 = a-a1/a0-a1. a-a2/a0-a2 = 1/6a2 - 3/2a +10/3
- l1 = a-a0/a1-a0. a-a2/a1-a2 = 1/2a2 + 7/2a – 5
- l2 = a-a0/a2-a0. a-a1/a2-a1 = 1/3a2 – 2a +8/3

Thus, H(z)= Hz = bj-lj(z)2j=0

=2383 (1/6z2 - 3/2z +10/3) + 2919 (1/2z2 + 7/2z – 5) + 3244 (1/3z2 – 2z +8/3)

H(z) = 1999 + 154z + 19z2

B. AES Algorithm

This symmetric encryption algorithm which is an iterative rather than Festal cipher. Substitution permutation network is the foundation of AES algorithm. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs i.e. substitutions and others involve shuffling bits around permutations.

1) Step 1: Select two Prime Numbers P and Q
2) Step 2: Compute N=p*q
3) Compute φ(N)=(p-1)*(q-1)
4) Step 3: Choose e such that 1<e and e are Co-prime
5) Step 4: Computer a value for d such that (d*e)% φ(N)=1
6) Step 5: Public key is (e, N) Private Key is (d, N)

C. Algorithm for fragmentation

Splits the file into number of block.

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
4) Size= size of source file
5) Fragments=size/Nof
6) End

Mathematical model

Let, $X=(x_1,x_2,x_3,x_4 \ldots\ldots\ldots\ldots x_B)$

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

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

for i=1,2,3……N

here N is sub-vectors

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

Be the data stored on CSP(Cloud Service 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, $Vi \geq 1$ and distinct for i ∈ 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

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

VI. RESULTS

Test Case	Expected Result	Actual Result
Registration with correct user details	User should be allowed to create new account	User was able to create new account
Registration with incorrect user details	User should not allowed to create new account and must display "incorrect details"	User was unable to create new account and message displayed as "incorrect details"
Login with correct username and password	User should be successfully login to account	User was able to login successfully
Login with incorrect username and password	User should not be allowed to login and must display "incorrect username and password"	Website application displayed "incorrect username and password"
Uploading file with valid file format	User should be allowed to upload file on cloud storage	Application allowed user to upload file on cloud storage
Uploading file with invalid file format	User should not be allowed to upload file on cloud storage	User not allowed to upload a file on cloud storage
Inserting correct secret keys	Application should allow user to download the required file	Access was given by the application to download the required file
Inserting wrong secret keys	Application should not allow user to download the required file	Access was denied by application to download the file
Sending auto mail consisting secret keys	Mail must be send to corresponding registered user	Mail has sent to the registered user

Table 1: Result Analysis

VII. CONCLUSION

The aim of this work is to study and secure the Multi-cloud with the help of secret sharing algorithm. This purpose is achieved implementing Shamir's secret sharing algorithm. This secret sharing scheme has a good foundation that offers an excellent platform for proofs and applications. From the consideration of all the above focuses, we displayed the structure that minimizes storage cost when the user stores his data in multiple clouds.

As far as most of existing work considers only data confidentiality and availability, while proposed methodology addresses the issue of data integrity in multiple clouds simultaneously with minimum cost this is a challenging problem.

REFERENCES

[1] Ping Hu, Chi Wan Sung, Siu Wai Ho, Terence H. Chan, Optimal Coding and Allocation for Perfect Secrecy in Multiple Clouds, IEEE Transactions on Information Forensics and Security, Vol. 11, No. 2, February 2016.
[2] Mazhar Ali, Athanasios V. Vasilakos,SeDaSC: Secure Data Sharing in Clouds, Fellow IEEE Syst. J.,to be published, doi :10.1109/JSYST.2014.2379646.
[3] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J., vol. 28, no. 4, pp. 656715, Oct. 1949.
[4] Ms.V.Mangaiyarkkaras and Mr. K. A. Dhamodaran, A Comparative Survey on Availability and Integrity Verification in Multi-Cloud, Volume 1, Issue 10, December 2012.
[5] Monica G. Charate, Dr. Savita R. Bhosale, Cloud Computing Security Using Shamirs Secret Sharing Algorithm From Single Cloud To Multi Cloud, Volume No 03, Special Issue No. 01, April 2015.
[6] Ang Li,Xiaowei Yang , CloudCmp: Comparing Public Cloud Providers, November 13, 2010, Melbourne, Australia.
[7] Marten van Dijk, Ari Juels , On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing, RSA Laboratories.
[8] Adla Shekhar, Janapati Venkata Krishna, Secure and Reliable Cloud Security from Single to Multi Clouds, volume 16 number 2 Oct 2014.
[9] L.Naveen Kumar, K.Kiran Reddy, Multi-Cloud Based Framework for Improved Service Availability and

Security, IJCTT,volume 5, number 4, ISSN: 2231-2803,Nov 2013
[10] A.Bessani,M. Correia, B.Quaresma, F.Andre and P.Soura Depsky:dependable and secure storage in cloud computing.2011.
[11] F.Rocha and M.Correia lucy in the Sky without Diamond: stealing Confidential Data in the Cloud, Proc 1stIntl. Workshop od Dependability of Clouds, Data Centres and Virtual Computing Environments, 2011.
[12] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.
[13] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.
[14] C. Cachin, R. Haas and M. Vukolic,"Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.
[15] E.Grosse, J.Howie, J.Ransome, J Reavis and S.Schmidt, Cloud computing roundtable, IEEE Security Privacy,8(6),2010.
[16] W.Itani, A.Kayssi, A.Chehab, Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures Eight IEEE International Conference on Dependable, Autonomic ans Secure Computing, Dec 2009.
[17] E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE Security Privacy, 8(6), 2010, pp. 17-23.
[18] N. Santos, K.P. Gummadi and R. Rodrigues, "Towards trusted cloud computing", USENIX Association, 2009, pp. 3-3.
[19] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium onCloud computing, 2010, pp. 229-240.
[20] A.J. Feldman, W.P. Zeller, M.J. Freedman andE.W. Felten, "SPORC: Group collaboration usinguntrusted cloud resources", OSDI, October2010, pp. 1-14.
[21] E. Grosse, J. Howie, J. Ransome, J. Reavis and S.Schmidt, "Cloud computing roundtable", IEEE Security Privacy, 8(6), 2010, pp. 17-23.
[22] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi,M. Dahlin and M. Walfish, "Depot: Cloud storagewith minimal trust", OSDI'10: Proc. of the 9thUSENIX Conf. on Operating systems design andimplementation, 2010, pp. 1-16.
[23] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y.Michalevsky and D. Shaket, "Venus: Verificationfor untrusted cloud storage", CCSW'10: Proc.ACM workshop on Cloud computing securityworkshop, 2010, pp. 19-30.
[24] K.D. Bowers, A. Juels and A. Oprea,"HAIL: Ahigh availability and integrity layer for cloudstorage", CCS'09: Proc. 16th ACM Conf. onComputer and communications security, 2009, pp.187-198.
[25] C. Cachin, I. Keidar and A. Shraer, "Trusting thecloud", ACM SIGACT News, 40, 2009, pp. 81-86. [15] Clavister, "Security in the cloud", Clavister WhitePaper, 2008.
[26] N. Santos, K.P. Gummadi and R. Rodrigues," Towards trusted cloud computing", USENIX Association, 2009, pp. 3-3.

