International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967 *Volume 2 , Issue 1(Jan-Feb 2015), PP1-5*

Secure Sharing Of Data in Cloud Computing With Secret Sharing Algorithm

Abhishek Chandan[1], Sahadev Gupta[2],RichaKumari[3],VrindaRajan[4,]Shubhangi Sonone[5]

*[1 2 3 4 5](Dr.D.Y.Patil College of Engineering, Ambi,Pune
Savitribai Phule Pune University)*

Abstract:- Cloud computing is an emerging technology which has considerable potential as an alternative process for traditional silo computing. One can deploy applications more speedily across shared server storage resource pools than with conventional enterprise solutions. Deploying modern web applications across a cloud framework enables a new level of agility that is very difficult to accomplish with traditional silo computing mode. Besides all the benefits concerned with cloud computing there is a big issue to be concerned which is its security, reason is involvement of third party. Nowadays enterprises wants to avoid an untrusted cloud movement so they prefer using multiple-clouds rather than single cloud provider. By keeping the importance of data into consideration this paper basically focuses on securing the relevant data using multicloud approach with the help of secrete sharing algorithm.

Keywords:- Cloud computing, DepSky Architecture, Multi-clouds, Secrete Sharing, Security

I. INTRODUCTION

DOPTING cloud computing can help organizations to conduct their core business activities more effectively Asince the managing and monitoring task for data centers is reduced. Again businesses can also save on power costs as the resources required are reduced. One may think if cloud computing is such a great thing then why most businesses are not going for it and as per the research the reason is poor security. The third party is involved called CSP (Cloud Service Provider) to whom businesses have to provide their data including sensitive data. This paper survey's recent research related to security of single and multi-cloud comes up with possible solutions for preservation of security. Though multi cloud computing is relatively new concept, biggest security factors in cloud computing such as data intrusion, data integrity, and service availability are handled in a better way in multi-cloud than single cloud computing .This project work promotes the use of multi-cloud architecture .In its broadest usage, the term cloud computing refers to the delivery of scalable IT resources over the Internet as divergent to hosting and operating those assets locally such as on a college or university network. Those resources can include claims and amenities as well as the infrastructure on which they operate. By organizing IT infrastructure and services over the network, an organization can acquire these resources on as-needed basis and avoid the capital costs of software and hardware. With cloud computing, IT capacity can be adjusted quickly and easily to accommodate changes in mandate. While remotely hosted managed services have long been a part of the IT landscape. A keen interest in cloud computing is being fueled by ubiquitous networks, growing standards, the rise of hardware and software virtualization and the push to make IT costs variable and transparent.

II. RELATED WORK

Literature survey

Research illustrates that in 2009, 67% of the research on security in cloud computing covered the issue of a single cloud, whereas 33% of the research in the same year covered the issue of multi-clouds. In 2010, 80% of research focused on single clouds while only 20% or research was directed in the area of multi-clouds [8].

HAIL (High Availability and Integrity Layer) which is combination of Proofs and cryptography, presented in the year 2009 used to control multiple clouds. It ensures data integrity and service implementation. But the limitation of HAIL is that it needs code execution in their servers and it does not deal with multiple versions of data [5].RACS (Redundant Array of Cloud Storage) is a protocol for intercloud storage in the year of 2010.This Technique is similar to RAID and normally used by disks and file systems and replication offers better fault tolerance. But the problem is unable to cooperate with vendor lock-in and economic failure. Cachin [11] presented a design for intercloud storage named ICStore in 2010. ICstore is client centric distributed protocol which can handle data integrity issue but has poor performance in case of data intrusion and service availability. Same thing happened with encrypted cloud VPN [4].

Moving from single clouds to multi-clouds is sensible and significant for many causes. According to Vukolic [15] accepts that the key purpose of moving to interludes is to amend what was offered in single clouds.

DepSky presented by Bessani [9] in 2011 is virtual storage cloud system comprising of a combination of different clouds to build a cloud-of-clouds. None of above complications are found in DepSky as it combines Byzantine fault tolerance protocol, secrete sharing and cryptography [16].

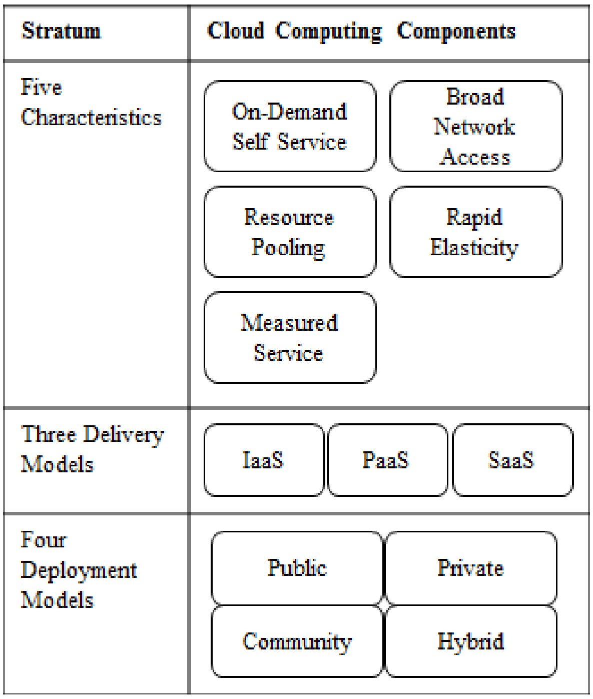
Background

NIST defined cloud computing as “a model for enabling appropriate,on-demand network access to a shared pool of configurable computing resources (e.g.,networks, servers, storage, claims, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

i. Cloud Computing Component

The cloud computing environment comprises of five features, three delivery models and four deployment models (see Fig. 1). The five important characteristics of cloud computing are comprising first stratum are: location-independent resource pooling that is provider resources pooled to server multiple clients, on-demand self-service, rapid elasticity which is ability to quickly scale in/out service, wide-ranging network access, and measured service that is renting the services use per pay basis.

Three Cloud Carriage models are Iaas,PaaS and SaaS, comprises middle stratum of cloud computing environment.



Stratum	Cloud Computing Components
Five Characteristics	On-Demand Self Service Broad Network Access Resource Pooling Rapid Elasticity Measured Service
Three Delivery Models	IaaS PaaS SaaS
Four Deployment Models	Public Private Community Hybrid

Fig. 1: Cloud Computing Environment

In Software as a Service(SaaS), applications are there that are enabled for the cloud. It ropes an architecture that can run multiple instances of itself which are location independent. This is nothing but a periodic subscription based pricing model and it is stateless. An example of SaaS are the Salesforce.com CRM application, MobileMe, Google docs, Zoho. This model represents the second layer in the cloud environment architecture.

Platform as a Service(PaaS) includes platform on which developers can write their applications to be run on cloud environment. This platform normally has multiple application services available for quick organization. Examples of PaaS are Google Application Engine, Microsoft AZURE and Salesforce.com.

Infrastructure as a Service (IaaS) used by consumer by providing storage, processing, networking, and other fundamental computing resources where the consumer is able to deploy and run software, which might include operating systems and applications. It is extremely scaled redundant and shared computing Infrastructure approachable using internet technologies. Specimens of this type of delivery model include Amazon web service.

III. IMPLEMENTATION DETAILS

Primary Objective of our work is to make the assurance that data is in secure and stable form. We are using DepSky system in our work which contains four commercial storage clouds(Amazon S3,Windows Azure, Nirvanix and Rackspace).It increases the system availability as data is not relayed on a single cloud, also avoids vendor lock-in issue since lack of dominant cloud. The DepSky system also reduces cost of than using single cloud, which is a significant advantage. DepSky uses a set of Byzantine quorum system protocols in order to implement the read and write operations in the system, so it needs only two communication round trips for each operation to deal with several clouds[4].To make a shift towards more secure cloud computing, we are using multi-cloud computing than that of single cloud computing.

a. DepSky Architecture

Bessani et al. [9] present a virtual storage cloud system called DepSky on which prototype of our system is based. As figure 2 shows it is a multi-cloud architecture which consists of a combination of different storage clouds. There are no codes to be executed as clouds are used for data storage and maintenance .The DepSky system accosts the confidentiality and the availability of data in their storage system.

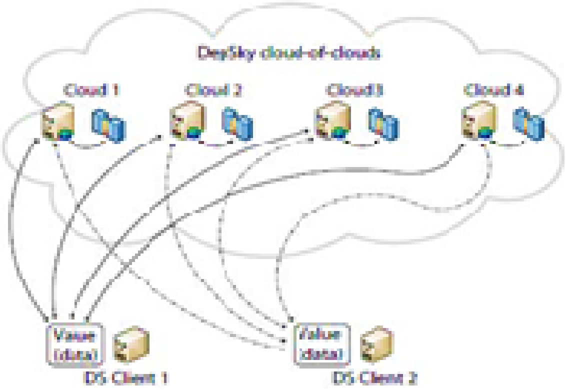


Fig. 2:DepSky Architecture

b. System Model of Depsky

It has readers, writers and cloud storage providers. Readers and writers are nothing but the client. As shown in fig 2, clouds 1-4 are cloud storage providers. A cloud storage provider does the tasks defined by readers and writers. Readers can fail irregularly, can crash and can present any behavior. But we cannot consider that writers can fail arbitrarily because of replicas. But replicas may be inconsistent, faulty writers may be able to write wrong valuesof data. To deal with this public key cryptography is used. Readers have access to public keys while common private key is shared by all writers of data unit. The DEPSKY algorithms are implemented as a software library in the clients.

c. Data Model of DepSky

DepSky library deals with different cloud interface providers as it is multi-cloud architecture. The data format DepSky should be acceptable by each cloud .Data model comprises of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation. The conceptual data unit contains a version number (to support updates on the object), verification data (usually a cryptographic hash of the data) and the data stored on the data unit object. Second level is generic data unit which has container for data, metadata and data object. Third abstraction level is data unit implementation in which container interpreted into the specific constructions supported by each cloud provider (Bucket, Folder, etc.). Four cloud providers are their which are Amazon S3, Windows Azure, Nirvanix and Rackspace.

IV. SECURITY USING SECRET SHARING

In our system we aim to provide a framework to supply a secure cloud database that will assure to prevent security risks that the cloud computing community is facing. This framework will go for multi-clouds architecture and the Shamir's secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity.

The scope of this project is to upload and download a file from multi-cloud.If one cloud is failed, we can download the same file from other cloud as the data is replicated among multiple clouds. Files should be uploaded using Byzantine fault tolerance (BFT) algorithm. The Byzantine protocols involve a set of storage clouds (n) where n = 3 f +1, and f is maximum number of clouds which could be faulty. In addition, any subset of (n – f) storage cloud creates byzantine quorum protocols [2], [9].

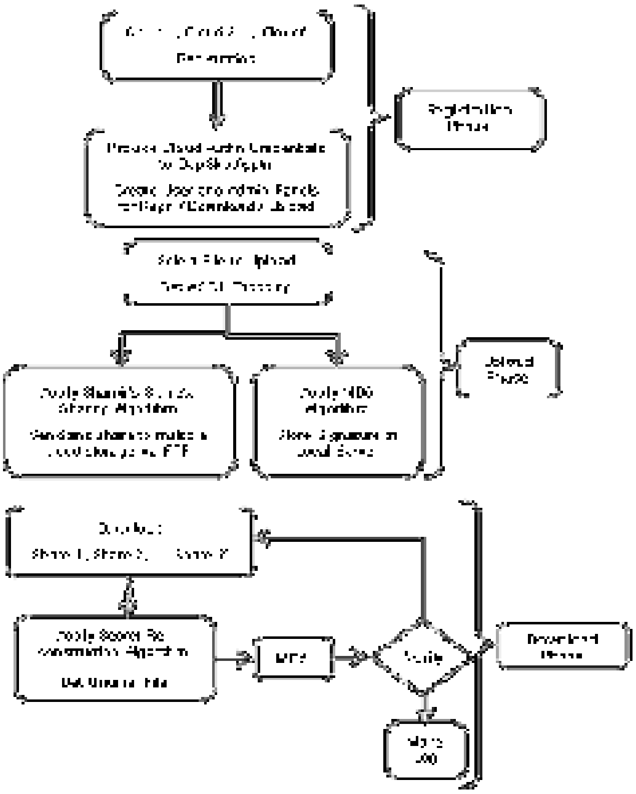


Fig.3. Block Diagram of Proposed System

Each file is encrypted and secrete generated. Next step in implementation is using Shamir's secrete sharing algorithm. In the Shamir's Secrete sharing scheme invented by Adi Shamir, secrete is divided into parts and then all parts are stored at different places (clouds in our case). So to reconstruct original secrete, one has to acquire all or some parts of thesecret from those different places [15]. Along with Shamir's secrete sharing scheme we are using Byzantine Fault Tolerance Protocol for deciding minimum number of parts of secrete require to generate original file. Message Digest concept MD5 is used for ensuring integrity of data at the time of upload phase as shown in figure 3.And at the time of download phase, reconstruction algorithm is applied to get original file and then verified with its message digest, if match found then file is considered to be integral.

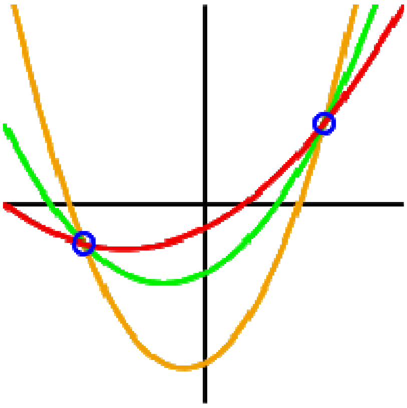
V. MATHEMATICAL MODEL

- Shamir's Secret Sharing[10] is an algorithm in cryptography created by Adi Shamir.
- It is a threshold scheme based on polynomial function technique.
- Secret is divided into parts, giving each participant its own unique or special part, where some of the parts or all of them are needed in order to reconstruct the secret
- The main goal associated with this scheme is to divide the following data D (e.g., the safe combination) into *n* pieces D*1*, D*2*…,D*n* in such a way that:
  - Knowledge of the value of any k or more Di pieces makes D easily computable.
  - Knowledge of any k-1value or fewer Di pieces leaves D completely undetermined.

Scheme
The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are adequate to define a parabola, 4 points are considered to define a cubic curve and so onwards. That is, it takes $k$points to define a polynomial of degree$k-1$.

Suppose we want to use a (k, n)threshold scheme to share our secret suppose$S$, without loss of generality assumed to be an element in a finite field$F$of size $P$where $0 < k \leq n < P; S < P$and $P$is a prime number.

Choose at random $k-1$positive integers $a_1, \cdots, a_{k-1}$with$a_i < P$, and let$a_0 = S$. Build the polynomial$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$. Let us construct any $n$points out of it, for instance set $i = 1, \cdots, n$to retrieve$(i, f(i))$. Every participant is given a point (an integer input to the polynomial, and the consistent integer output). Given any subset of $k$of these pairs, we can discover the coefficients of the polynomial using interpolation. The secret is the constant terma_0.



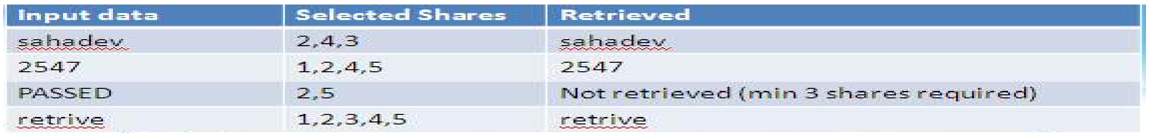
One can draw an infinite number of polynomials of degree 2 through 2 points. 3 points are required to define a unique polynomial of degree 2. This image is for illustration purposes only — Shamir's scheme uses polynomials over a finite field, not represent able on a 2-dimensional plane.

EXAMPLE:

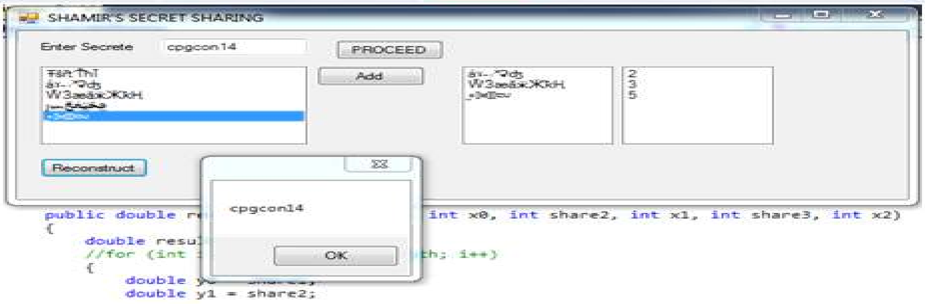
- Let S=1234

- 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)
- In order to reconstruct the secret any 3 points will be enough.

VI. EXPECTED OUTCOME



Input data	Selected Shares	Retrieved
sahadev	2,4,3	sahadev
2547	1,2,4,5	2547
PASSED	2,5	Not retrieved (min 3 shares required)
retrive	1,2,3,4,5	retrive



Enter Secrete: cpgcon14

2
3
5

cpgcon14

```
public double r                    int x0, int share2, int x1, int share3, int x2)
{
    double resu
    //for (int                     th; i++)
    {
        double y
        double y1 = share2;
```

VII. CONCLUSION AND FUTURE SCOPE

It is clear that although the use of cloud computing has swiftly increased, cloud computing security is still considered the major issue in the cloud computing atmosphere. Customers do not want to lose their private information as a result of malicious insiders in the cloud.

In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads too many problems for the users of cloud computing. The determination of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions.

We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multicloud have received less attention in the area of security. We support the relocation to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

VIII. ACKNOWLEDGEMENT

Every single engineering student looks toward the final year project as an opportunity by which he/she can implement the skill that he/she has eventually nurtured in the year by hard work dedication, the milestone of completing the project would have been intractable without the help of few people who need to be acknowledge. We take this opportunity to thank all those, who have subsidized to the accomplishment of this work and helped us with their valuable suggestions for improvement.

We express our deep gratitude to our guide, HOD and Principal from Dr. D Y Patil COE, Ambi,for their cherished support, help & guidance during the project work & providing us with best facilities and atmosphere for the inspired work, guidance and encouragement.

REFERENCES

[1] (NIST), http://www.nist.gov/itl/cloud/

[2] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.

[3] 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.

[4] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-clouds," hicss, pp.5490-5499, 2012 45th Hawaii International Conference on System Sciences, 2012.

[5] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp. 187-198.

[6] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[7] Cong Wang1, Qian Wang1, Kui Ren1, and Wenjing Lou2," Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing",IEEE INFOCOM 2010, San Diego, CA, March 2010

[8] K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80.

[9] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.

[10] Shamir, A.: How to share a secret. Communications of the ACM, 612–613 (1979).

[11] Clavister, "Security in the cloud", Clavister White Paper, 2008.

[12] I. Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory",Distributed Computing, 18(5), 2006, pp. 387-408.

[13] S. Kamara and K. Lauter, "Cryptographic cloud [41] storage", FC'10: Proc. 14thIntl.Conf. On Financial cryptography and data security, 2010, pp. 136-149.

[14] G.R. Goodson, J.J. Wylie, G.R. Ganger and M.K. Reiter, "Efficient Byzantine-tolerant erasure-coded storage", DSN'04: Proc.Intl. Conf. on Dependable Systems and Networks, 2004, pp.1-22.

[15] E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), 2010, pp. 17-23.

[16] J. Hendricks, G.R. Ganger and M.K. Reiter, "Low-overhead byzantine fault-tolerant storage", SOSP'07: Proc. 21st ACM SIGOPS symposium on Operating systems principles, 2007, pp. 73-86