Single to Distributed Cloud Computing Security

Neha N. Latpate
Sinhgad Institute of technology, Lonavala, Maval, Pune-410401

S.B. Waykar
Sinhgad Institute of technology, Lonavala, Maval, Pune-410401

ABSTRACT
It is the actual concern of the cloud's, because of it's easy nature as a shared resource, identity management, privacy and access management. it is additional confidential issue give to provide correct security and different probably vulnerable areas became a priority for organizations acquiring with a cloud computing provide,.and it's relating to With additional organizations exploitation cloud computing and associated cloud suppliers for information operations.

you may feel forced in your ability to barter through business disagreements with their provider,only when If crucial information and applications square measure obsessed with one cloud provider. This paper addresses doable solutions, for that surveys that is recent analysis associated with single and multi-cloud security. it's found that the analysis into the employment of multi-cloud suppliers to keep up security has received less attention from the analysis community that has the employment of single clouds. owing to its ability to scale back security risks that have an effect on the cloud computing user, this work aims to push the employment of multi-clouds.

Keywords
Cloud computing, Security, Distributed Cloud, single to multi cloud environment.

1. INTRODUCTION
Because of the service provider will access the information that's on the cloud at any time Cloud computing poses privacy considerations. It might accidentally or deliberately alter or perhaps delete data. If necessary for functions of law and order even while not a warrant, several cloud suppliers will share data with third parties. That's permissible in their privacy policies that users have to be compelled to comply with before they begin victimization cloud services. Solutions to privacy embrace policy and legislation similarly as finish users' selections for a way information is keep.

Dealing with "single cloud" as a result of potential issues like service accessibility failure and also the chance that there are malicious insiders within the single cloud, suppliers is changing into less fashionable customers. In recent years, there has been a move towards "multi-clouds", "inter-cloud" or "cloud-of-clouds"...

The cloud computing model consists of 5 characteristics, 3 delivery models, and 4 preparation models. The 5 key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, fast snap, broad network access, and measured service.

The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Infrastructure as a service is taking the physical hardware and going utterly virtual (e.g. all servers, networks, storage, and system management all existing within the cloud). this can be the love infrastructure and hardware within the ancient (non-cloud computing) methodology running within the cloud. In different words, businesses pay a fee (monthly or annually) to run virtual servers, networks, storage from the cloud. for an information center, heating, cooling, and maintaining hardware at the native level, this may mitigate the requirement. Platform as a service is cloud computing service that provides the users with application platforms and databases as a service. this can be equivalent to middleware within the ancient (non-cloud computing) delivery of application platforms and databases.The software-as-a-service (SaaS) service-model involves the cloud provider putting in and maintaining code within the cloud and users running the software from their cloud clients over the net (or Intranet). The users' client machines need no installation of any application-specific code - cloud applications run on the server (in the cloud). SaaS is scalable, and system administration might load the applications on many servers.

Cloud deployment models embrace public, private, community, and hybrid clouds. a public cloud, could be a cloud environment that's accessible for multi-tenants and is available to the general public. a non-public cloud is on the market for a selected cluster, whereas a community cloud is changed for a selected cluster of consumers. composition of 2 or additional clouds (private, community, or public cloud) is termed Hybrid cloud infrastructure. This model represents the third layer within the cloud environment design.

By adopting a multi-cloud strategy, that is, by running your cloud-based deployments on different cloud providers, redundancy is taken to a full new level. By choosing information centers from completely different providers to host our cloud servers, we are able to effectively eliminate the danger related to the business continuity of the infrastructure supplier, likewise as risks associated with electricity suppliers, networking suppliers and different "data center" problems, since every cloud provider can typically operate individually.

Other risks related to having one provider reduces a multi-cloud strategy: to Illustrate somebody discovers a vulnerability on the virtualization platform that your current infrastructure provider uses. If you're deploying on multiple clouds, you'll be able to merely shut down the servers on the vulnerable provider with very little or no impact to your operations. a similar mentality applies if suddenly your provider decides to extend its costs, or perhaps modification its terms of service: stop working your servers, and move your business to somebody else.

Multi-cloud strategy is that the use of 2 or a lot of cloud to reduce the danger of service accessibility failure, Loss and corruption of knowledge, loss of privacy, seller lock-in and also the chance of malicious insiders within the single cloud. The service inconvenience will occur owing to breakdown of hardware, code or system infrastructure. A multi-cloud strategy may also improve overall enterprise performance by avoiding "vendor lock-in" and exploitation completely different infrastructures to satisfy the requirements of

numerous partners and customers. the price of exploitation multiple clouds are going to be more than that of single clouds. so unless and till there's a style which might build use of multi-clouds while not increasing price, the implementation are going to be extremely impractical.

2. LITERATURE SURVEY

D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", The technical contributions of this paper is the establishment and development of a framework for efficient fault-tolerant scalable and theoretically secure privacy preserving data outsourcing that supports a diversity of database operations executed on different types of data, which can even leverage publicly available data sets.

G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", We present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data.

A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", In this paper we present DEPSKY, a system that improves the availability, integrity and confidentiality of information stored in the cloud through the encryption, encoding and replication of the data on diverse clouds that form a cloud-of-clouds.

C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Inter cloud", we discuss the design of Interclouds storage, which we currently are implementing, as a primer for dependable services in the Interclouds. Interclouds Storage precisely addresses and improves the CIRC attributes (confidentiality, integrity, reliability and consistency) of today's cloud storage services.

C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", We analyze the problem of efficient distributed storage of information in a message-passing environment where both less than one third of the servers, as well as an arbitrary number of clients, might exhibit Byzantine behavior, and where clients might access data concurrently

A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using Untrusted cloud resources", Conceptually, SPORC illustrates the complementary benefits of operational transformation (OT) and fork* consistency. The former allows SPORC clients to execute concurrent operations without locking and to resolve any resulting conflicts automatically.

3. PROPOSED APPROACH FRAMEWORK AND DESIGN

3.1 Architecture

At Present a virtual storage cloud system known as DepSky that consists of a mix of various clouds to make a cloud-of-clouds are used. The DepSky system addresses the provision and also the confidentiality of information in their storage system by victimisation multi-cloud providers, combining Byzantine assemblage system protocols, science secret sharing and erasure codes DepSky is one such design style that overcomes all the restrictions of multi-clouds by eliminating the need of code execution within the servers (i.e., storage clouds). it's still economical because it needs solely 2 communication round-trips for every operation. Also, it deals with knowledge confidentiality and reduces the quantity of information keep in every cloud. It uses associate degree economical set of Byzantine assemblage system protocols, cryptography, secret sharing, erasure codes and also the diversity that comes from exploitation many clouds. The DepSky system model contains 3 parts: readers, writers, and 4 cloud storage providers, wherever readers and writers square measure the client's tasks. The DepSky protocols give consistency proportional linguistics, i.e., the linguistics of an information unit is as sturdy because the help clouds permit, from ultimate to regular consistency linguistics. to make sure confidentiality of keep knowledge on the clouds while not requiring a key distribution service, we tend to use a secret sharing theme.

The DepSky design consists of 4 clouds and every cloud uses its own explicit interface. The DepSky rule exists within the clients' machines as a software package library to speak with every cloud (Figure 2). These four clouds square measure storage clouds, thus there aren't any codes to be executed. The DepSky library permits reading and writing operations with the storage clouds.

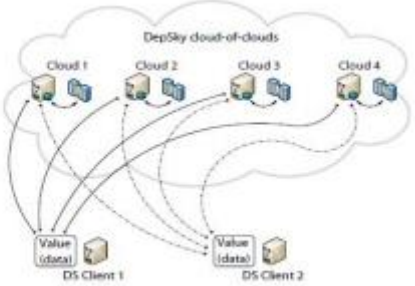


Figure 2: DepSky Architecture

3.2 Algorithm

A. Algorithm for Data Integrity Verification

Step 1: Start
Step 2: TPA Generates a random set
Step 3: CSS computes root hash based on the filename/blocks input
Step 4: CSS computes the originally stored value.
Step 5: TPA decrypts the given content and compares with generated root hash.
Step 6: after verification, the TPA can determines whether the integrity is breached.
Step 7: Stop.

3.3 Mathematical Model

The mathematical implementation of Cloud Computing security algorithm can be understood with the help of a simple example. The generalized idea is as follow:

We choose at random (k-1) coefficients i.e. a1…ak-1 we divide our secret data 'S' by picking a random degree polynomial

$$q(x) = a0 + a1x1 + a2x2 + \cdots + ak - 1xk - 1$$

Where a0='S' (i.e. the data).

Now if we wish to divide the data into n parts, we will substitute 'n' different values of x in the polynomial q(x) and obtain 'n' such sets of (x, y), here y is nothing but our polynomial q(x).The essential idea of Aid Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes "k" points to define a polynomial of degree "k-1".

Select "k" such sets, any k combination of the available n parts will generate the same result. The value in these sets are meaningless alone, it is only when 'k' sets are brought in together and further worked upon that we get our secret back. These "k" instances of original polynomial are processed using Lagrange polynomials

The Lagrange basis is:

$$I0 = \frac{X-X1}{X0-X1}.\frac{X-X2}{X0-X2}$$

$$I1 = \frac{X-X0}{X1-X0}.\frac{X-X2}{X1-X2}$$

$$I2 = \frac{X-X0}{X2-X0}.\frac{X-X1}{X2-X1}$$

Substitute the values of x from the selected 'k' sets into the Lagrange basis and we obtain 'k' fractional equations for the same. Finally on taking summation of the equations obtained from Lagrange basis and y form the selected 'k' sets, we get back our original polynomial. The summation can be represented mathematically as:

$$f(x) = \sum_{j=0}^{2} y_j \,.\, I_{j(x)}$$

The above explanation helps in understanding the working of the secret sharing algorithm. When done manually the entire calculation can be done in minutes, while on implementation, as the microprocessor technology has elevated its level to a new high, thousands of such calculations can be done in seconds.

4. WORK DONE

In this section we are discussing the practical environment, scenarios, performance metrics used etc.

4.1 Input

In this user signature is the input for our practical experiment.

4.2 Hardware and Software Configuration

Hardware Requirements:

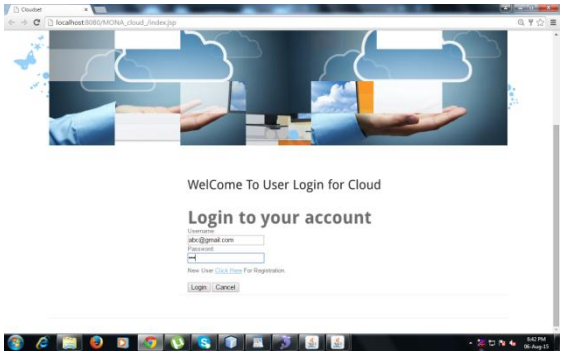
- Processor : Pentium IV 2.6 GHz
- RAM :512 MB DDR RAM
- Hard Disk : 20 GB

Software Requirements:

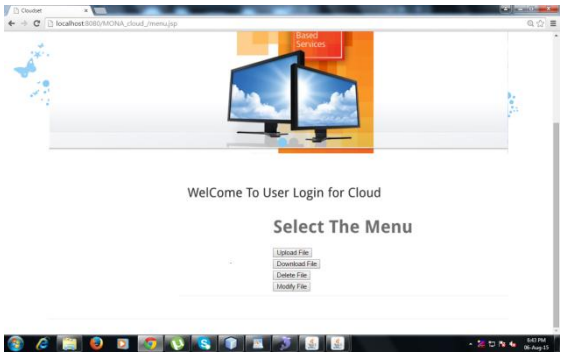
Front End	: Java
Tools Used	: NetBeans
Operating System	: Windows 7/8
Database	: MySQL

4.3 Results

Results are shown below:



Enter username and password and click on login button.



After login you will see this window.

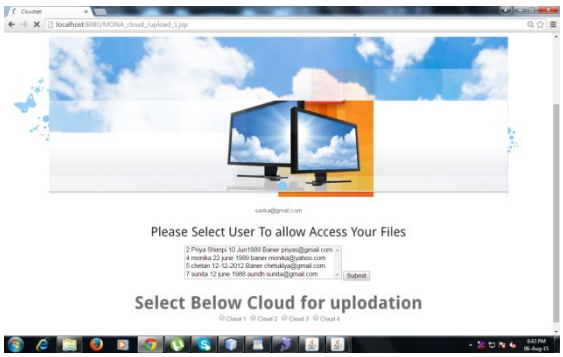
Here select the menu.

To upload file click on Upload File.

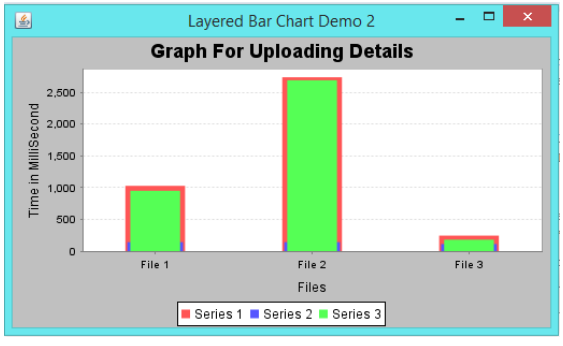
To Download file click on Download File.

To delete file click on delete file.

To modify file click on Modify file.



Here select user to allow access to your files and select cloud for upload.



The result graphs are as shown above.

5. CONCLUSION AND FUTURE WORK

The use of cloud computing has been quickly augmented however the most important issue within the cloud computing environment continues to be in thought. from malicious corporate executive within the cloud, the users perpetually wish their information to be secure . several drawback for an oversized range of consumers recently caused by the loss of service convenience. what is more, for the users of cloud computing information intrusion leads to several issues. Our main purpose is to understand concerning security risks and solutions of single clouds and multi-clouds There search has been done to make sure the safety of the only cloud and cloud storage wherever multi-clouds have received less attention within the space of security. we tend to support the migration to multi-clouds as a result of its ability to decrease security risks that have an effect on the cloud computing user.

6. REFERENCES

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

[2] 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.

[3] H. Abu-Libdeh, L. Prince House and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[4] D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.

[5] M.A. AL Zain and E. Paredes, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[6] Amazon, Amazon Web Services. Web services licensing agreement, October3, 2006.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.

[8] 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.

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

[10] 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.

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

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

[13] C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", DISC: Proc.19thIntl.Conf. On Distributed Computing, 2005, pp. 497-498.

[14] M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998, pp. 173-186.

[15] G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer, 42, 2009, pp. 60-67.

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

[17] A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October2010, pp. 1-14.

[18] S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?" IEEE Security and Privacy, 1(6), 2003, pp. 20-26.

[19] S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Cite seer, 2007, pp. 1-15.

[20] E. . . Goh, H. Shacham, N. Modadugu and D. Boneh, "SiRiUS: Securing remote untrusted storage", NDSS: Proc. Network and Distributed System Security Symposium, 2003, pp. 131–145