Ensuring Security in Multi-Cloud Computing

Y. Madhusekhar[1], Snehal P. Rokade[2]

[1]Assoc. Professor Computer Science Department, R R S College of Engineering & Technology
Muthangi (Vill), Patancheru (Mdl),Hyderabad, Andhra Pradesh, India, Pin- 502 300

[2]M.Tech Computer Science Department, R R S College of Engineering & Technology
Muthangi (Vill), Patancheru (Mdl),Hyderabad, Andhra Pradesh, India, Pin- 502 300

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 is possible 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 computin . Rather than this all the benefits of cloud computing has big issue to be concern which is its security, reason is involvement of third party. Now a day's enterprises preferring "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" rather than single cloud provider. Focal point of this paper is multicloud security by using secrete sharing algorithm.***

Keywords: Cloud Computing, Multi-clouds, DepSky Architecture, Secrete Sharing security, Fault Tolerance.

1. Introduction

Adopting cloud computing can help organizations to their conduct core business activities more effectively since the managing and monitoring task for data storage & centers is reduced. Again businesses can also save on power costs as per the resources required are reduced. Then 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 surveys recent research related to security of single and multi-cloud and comes up with possible solutions for preservation of security. Though multi-cloud computing is relatively new concept, biggest security factors in cloud computing domain, such as data integrity, data intrusion and service availability are controlled in better way in multi-cloud than that of single cloud computing [4]. This project work assists the use of multi-cloud architecture than that of single cloud architecture.

2. Background

NIST defined cloud computing as "a model for enabling convenient environment, on-demand network access to a shared pool of configurable computing resources (e.g., networks, applications, servers, storage and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[1]

- Cloud Computing Components

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

Figure 1: Cloud Computing Environment

The cloud computing environment constitute of five characteristics then 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, measured service and broad network access service that is renting the services use per pay basis.

Three Cloud Delivery models as IaaS, PaaS and SaaS, which comprises middle stratum of cloud computing environment. In Software as a Service (SaaS), applications are there that are enabled for the cloud. It provides an architecture that can run multiple instances of it which are location independent. This is just like a monthly subscription based pricing model and it is stateless. Google docs, MobileMe and Zoho are examples of SaaS.

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 deployment. Microsoft AZURE, Google App Engine and Force.com are examples of PaaS.

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 application, which can include operating systems environment and applications. It is highly redundant and shared computing Infrastructure approachable using internet technologies. Amazon EC2, Sun's cloud services and Terremark cloud offering this type of services.

Third stratum in the cloud computing environment consists of cloud deployment models which consist of public clouds, private clouds, and hybrid and community clouds. A cloud architecture which can be used by multi-tenants and is available to the public is called a public cloud. Cloud which is available for a specific group is private cloud, while a community cloud is modified for a specific group of users. Hybrid cloud is a combination of two or more clouds [4].

3. 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 inter-clouds. It provides data integrity and service availability. But some limitations of HAIL are 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 inter-cloud 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. Similar case happened with encrypted cloud VPN [4].

We will discuss three security factors that particularly affect single clouds, namely data integrity, data intrusion, and service availability.

3.1. Data Integrity

Data integrity is one of the most important issues related to cloud security risks. The data which stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachin al. [6] give examples of the risk of attacks from both inside and outside the cloud service provider, such as recently attacked Red Hat Linux's distribution servers [40]. As a solution, Cachinet al. [6] suggests that using Byzantine fault-tolerant protocols across multiple clouds from different providers is a beneficial solution.

3.2. Data Intrusion

According to Garfinkel [19], another security risk which occurs with a cloud service provider, such as the Amazon cloud service, which cloud service, is a hacked password or data intrusion. If someone gains access rights of an Amazon account password, they will be able to access all instances and resources of that account. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify information, or even disable its services.

3.3 Service Availability

Service availability is another major concern in cloud services. As Amazon mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's service may terminate for any reason at any time if any user's files break the cloud storage policy. Moving from single clouds multi-clouds is sensible and significant for many reasons. As per Cachin et al [5], "Services of single clouds are still subject to outage". Vukolic [15] accepts that the primary aim of moving to inter-clouds 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. These problems are not found in DepSky as it combines Byzantine fault tolerance protocol, secrete sharing and cryptography [16].

4. 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 requires 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 instead of single cloud computing.

- **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.

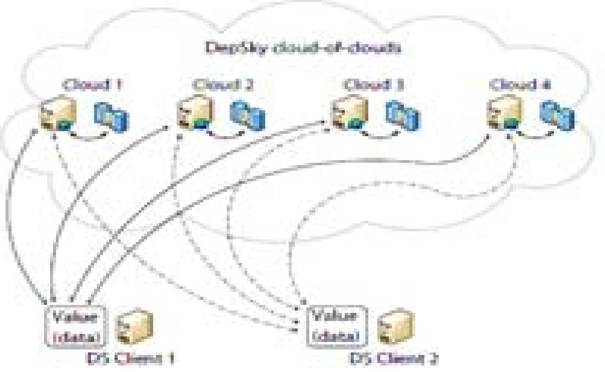

Figure 2: DepSky Architecture

- **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. The tasks defined by readers and writers are carried by cloud storage providers. Readers can fail irregularly, can crash and can present any behavior. But we cannot consider that writers can fail arbitrarily because of replicas. But these replicas may be inconsistent, faulty writers may be able to write some wrong values of data. To make it secure public key cryptography is used. Readers can access these public keys where as common private key is shared by all writers for unit of data. The DEPSKY algorithms are implemented as a software library in the clients.

- **Data model of Depsky**

DepSky library deals with different cloud interface providers as it is multi-cloud architecture. The data format of DepSky should be acceptable by each cloud .Data model comprises of three abstraction levels as the conceptual data unit, a generic data unit, and implementation data unit. 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 of abstraction is generic data unit which has container for data, metadata and data object. Data unit implementation is third abstraction level in which container interpreted into the specific constructions supported by each cloud provider (Bucket, Folder, etc.).

- **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].

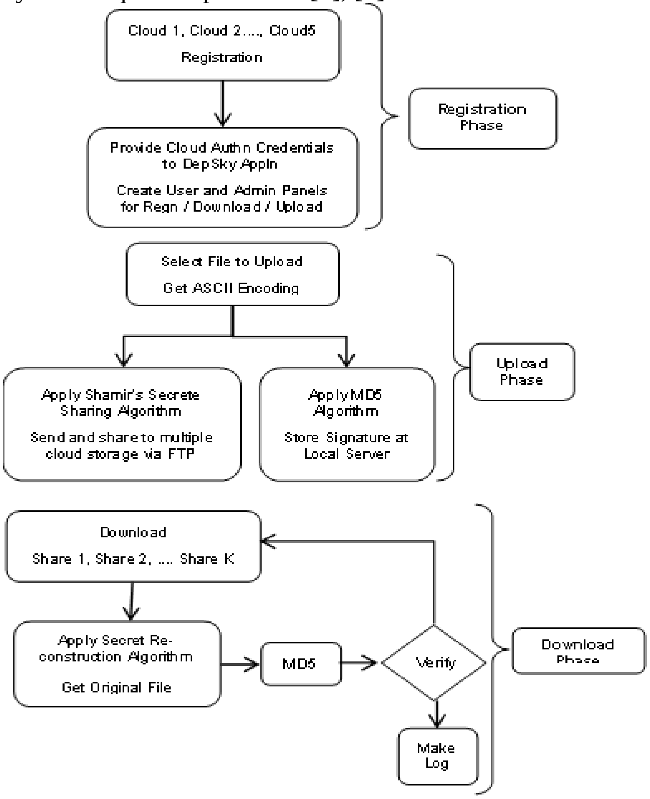
Cloud 1, Cloud 2...., Cloud5
Registration
Provide Cloud Authn Credentials to DepSky Appln
Create User and Admin Panels for Regn / Download / Upload
Registration Phase
Select File to Upload
Get ASCII Encoding
Apply Shamir's Secrete Sharing Algorithm
Send and share to multiple cloud storage via FTP
Apply MD5 Algorithm
Store Signature at Local Server
Upload Phase
Download
Share 1, Share 2, ... Share K
Apply Secret Re-construction Algorithm
Get Original File
MD5
Verify
Make Log
Download Phase

Figure 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, need to acquire all or some parts of the secrete key from those different places [15]. 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.

5. Result

Data set for this system is trusted users file to upload or download to the cloud or upload or download from the cloud. The result for this system is retrieval of same file in secure manner, reducing the risk of data intrusion and preserving integrity of the file.

Three modules are there in our system admin module, member module and secrete sharing module. Admin can create, Edit and delete Member details. Admin can configure the cloud details. Admin can also set the fault tolerance and provide number of clouds to Member for upload the file. Admin can able to view transaction details of member.

Member has to Login with their user Id and password. He can view his own profile. Member has rights to upload the file in multi-cloud. Before uploading, he has to create MD5 for that file and save it in database. Member can download the file from Cloud and save that file in local system and also has to create MD5 for downloaded file. Compare MD5 form database and MD5 file from local system. Both MD5 are equal integrity status is true (i.e., File is not corrupted) or else failed (i.e. File is corrupted).He can view only his transaction details and change his password.

There are many secrete sharing schemes are exist, but we used strongest secrete scheme mechanism that is Shamir’s secrete sharing scheme [10]. Though it has more complex computations it gives better confidentiality. It does not give any knowledge about original data to CSP also. While making a cloud secure, the following objectives are fulfilled:

- Understanding environment of the cloud computing provided by the cloud service provider
- The solution of cloud computing should meet the basic security & privacy requirements of any firm deploying it.
- Maintain an account of the privacy of the cloud& data security and applications that are deployed in cloud computing environment
- Data Integrity preservation
- Increased Service Availability
- Using service provider’s resources user runs customer applications.

6. Conclusion and Future Scope

Use of cloud computing has rapidly growing but with major issues to be taken care is cloud security [11]. Security is the reason due to which most of the businesses hesitating for moving their workload to cloud computing. Cloud clients fear to lose their private information if malicious insiders in the cloud. Also service availability is area to be concerned in single cloud, if that cloud fails [17]. In multi-cloud data is replicated so available even if on cloud fails. Integrity of data is also maintained in our proposed work by making use of MD5.We are making use of strongest cryptographic algorithm named Shamir’s secrete sharing algorithm, which has number of advantages including security, client-side aggregation. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multi-clouds have received less attention in the area of security. We affirm the moving to multi-clouds due to its ability to decrease security risks that affect the cloud computing user. The key conclusion is that proposed work provides data integrity, confidentiality, improved service availability and capacity to handle multiple requests at a time.

In future scope, we aim to implement privacy-preserving public auditing system for data storage security instead of verifying file at each upload and download phase by using its message digest (MD5). Storage auditing will be performed by TPA without demanding the local copy of data. Homo-morphic authenticator and random mask technique is used. This process eliminates the burden of cloud user from the tedious and possibly expensive auditing task. Proposed schemes will focused on economies of scale for Cloud Computing [7].

Reference

[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 & 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 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,
[17] L. Lamport, R. Shostak and M. Pease, "The Byzantine generals problem", ACM Transactions on Programming Languages and Systems, 4(3), 1982, pp. 382-401.
[18] F. Schneider and L. Zhou, "Implementing trustworthy services using replicated state machines", IEEE

Security and Privacy, 3(5), 2010, pp. 151-167.

[19] M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41, 2010, pp.105-111.

Author Profile

Mr. Y. Madhusekhar is working as Associate Professor Computer Science Department, R R S College of Engineering & Technology, Muthangi (Vill), Patancheru (Mdl), Hyderabad, Andhra Pradesh, India, Pin- 502 300

Snehal Rokade received the B.E. IT from MIT College of Engineering, Pune University in 2011 and M-Tech Computer Science degree from JNTUH in 2014. She is working with PES Modern College of Engineering, Pune as an Assistant Professor.