Cloud Computing Security Improvement using Secret Sharing Algorithm

Swapnila S Mirajkar[1], Shweta R.Kakade[2]
[1, 2] Department of Computer Engineering
[1, 2] JSPM's RSCOE, Pune

Abstract- *Cloud Computing is recently emerged as a service program, where users can remotely depot their data into the cloud so as to take advantage of on-demand high quality services from a shared pool of configurable computing resources. Cloud computing it 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 it also enables a new level of agility. Beside this, users will not have physical ownership of the outsourced data of possibly large size, hence the data integrity preservation in Cloud Computing is difficult task. Surveys on cloud computing imply that there should be proper privacy and security means for cloud, otherwise this may be disappointing. The term "multi-clouds", can be vied as an solution for improved data security by using secret sharing algorithm.*

Keywords- Cloud computing, Multi-Clouds, Secret Sharing Algorithm, MD5, Security

I. INTRODUCTION

The advancement of cloud computing environment is promoting many organizations to migrate their IT infrastructure to function completely or partially in the cloud. Acquiring cloud computing can help organizations to conduct core business activities more effectively and economically as the managing and monitoring task for data centres is reduced. As per NIST cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider communication [1]. The third party is called CSP(cloud Service Provider) is involved to whom businesses have to provide their data including sensitive data by which security risk is increased so there should be strong security mechanism .Paper lists various security challenges in cloud computing. The move towards more secure multi-cloud environment is motivated instead of trusting single cloud providers. Cloud solutions also allow you to hire extra processing power in the cloud for just a fraction of what you will have to pay for having all this infrastructure running in your company.

II. BACKGROUND

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

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

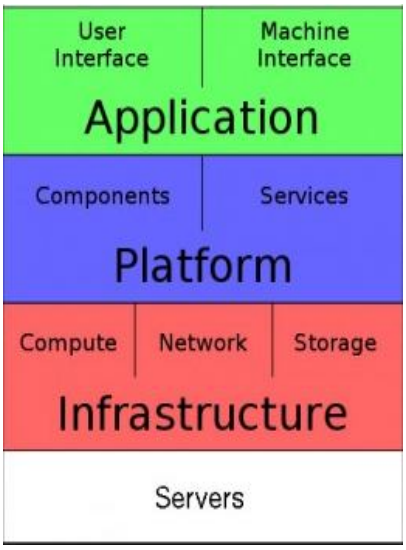

Fig. 1 Cloud Computing Environment

In Software as a Service(SaaS), applications are there that are enabled for the cloud. It supports an architecture that can run multiple instances of itself which are location independent. This is nothing but a monthly subscription based pricing model and it is stateless. Examples of SaaS are MobileMe, Google docs, Zoho.

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. Examples of PaaS are Google App Engine, Microsoft AZURE, Force.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 can include operating systems and applications. It is highly scaled redundant and shared computing Infrastructure approachable using internet technologies. Examples of this type of delivery model include Amazon EC2, Sun's cloud services etc.

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

III. NEED FOR CLOUD SECURITY

Adopting cloud computing involves many security related difficulties. The security requirements for cloud computing providers would appear to be the same as traditional data centres at first glance. Internet security problems will affect the cloud, with greater risks due to valuable resources stored within the cloud and cloud vulnerability. The technology used in the cloud is similar to the technology used in the Internet. The following abstracts some of the primary security concerns that enterprises should think about when planning their cloud computing deployment.

Clavister et al. [12], in their paper accomplished survey on the issues related to security in cloud computing. Besides of the great technological and cost effective advantages cloud computing has, businesses still think of the potential security threat before committing their data. Security is the most essential aspect of everyday computing; this is very well applicable to cloud computing itself. Few of the security concerns can be listed as follow:

A. Service Hijacking

Service hijacking is obtaining unauthorized services. Various techniques like fraud, phishing and software exploitation are included in this.

B. Malicious Attacker

There is cluster of data on cloud which attracts hackers. Hackers have become advanced these days to breach the strongest security provisions and hack crucial data. Attacker can inject viruses or worms into the database, and corrupt valuable information of the organization.

C. Virtual Machines Attacks

Cloud computing servers use the same web applications as localized virtual machines and same operating systems. Data and information of user is stored on virtual machines by cloud service provider. The ability for an attacker to remotely exploit exposures in these systems and applications is a substantial threat to virtualized cloud computing environments. In addition, locating multiple virtual machines at a place increases the attack extent and risk of VM-to-VM compromise.

D. Securing Hibernating Virtual Machines

When a virtual machine is offline, it is still available to any application that can access the virtual machine storage over the network unlike a physical machine, and is therefore capable to malware infection. However, dormant VMs do not have the capability to run an antimalware scan.

E. Application Security

As clouds provide the services and applications over internet, so there security is to be taken into consideration because user provides their information for accessing application. Hence, security of the applications is a necessity in cloud Computing.

IV. MULTI-CLOUD STRATEGY

As specified by Vukolic[6] the term multi cloud is "cloud of clouds - which says that the term cloud computing should not end up as a single cloud". Using their example, a cloudy sky comprises of different colours and shapes of clouds which leads to different executions and administrative domains.

Using single cloud there may be lack of availability of a service or valuable data at any point of time and that single cloud cannot prevent from possible loss. This can be reduced by using replication of resources; the same strategy is applied for multi-cloud application, in which storage of valuable resources are done at multiple clouds. This concept is getting popularity by organizations these days. Also trusting a

single cloud is risky as there could be some malicious user or software who is spying on the data being exchanged. So, to deal with these issues multi cloud environments have gained importance.

As per Cachin et al.[10], it is hard to address the data corruption issue, when number of clients use same cloud storage. The solution suggested is to make use of a Byzantine fault-tolerant replication protocol within the cloud. Any fault in cloud computing, which produces faulty output is called as Byzantine fault. Applying the Byzantine fault-tolerant replication protocol inside the single cloud is unsuitable due to the concept, that the servers belonging to cloud providers are physically located in the same place and uses the same system installations. So multi-cloud can be used to deal with Byzantine faults.

A. Multi-cloud Model :DepSky

The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers, aggregating Byzantine quorum system protocols, erasure codes and cryptographic secret sharing. We are applying DepSky model in our work which increases the resource availability as data is not relayed on a single cloud, also avoids vendor lock-in issue since lack of dominant cloud. DepSky architecture contains four commercial storage clouds(Amazon S3,Windows Azure, Nirvanix and Rackspace). The DepSky system is also economical. DepSky uses a set of Byzantine quorum system protocols in order to carry out read and write operations in the system, so it needs only two communication round trips for each operation to deal with several clouds[9].To make a shift towards more secure cloud computing, we are using multi-cloud computing than that of single cloud computing.

B. DepSky Architecture

Bessani et al. [9] present a virtual storage cloud system called DepSky on which prototype of our system is based. As fig.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.

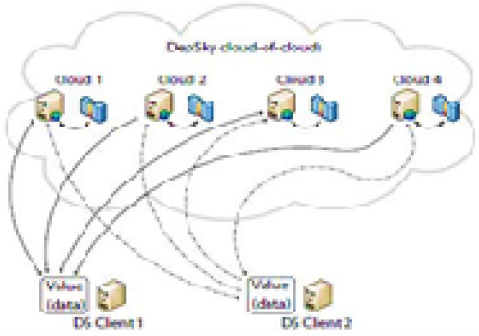

Fig.2 DepSky Architecture

F. 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 behaviour. 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 values of 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.

G. 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.).

V. PROCESS OF SHARING SECRET IN MULTI-CLOUD ENVIRONMENT

There may be case that data is lost due to some disaster befalling the cloud service provider. So we can replicate data on more than one cloud. We can apply encrypt technique before uploading data to the cloud. Again each cloud will have the same file, which is not secure. So here secret sharing algorithm can be to reduce the risk of data

intrusion and the loss of service availability in the cloud. Whenever user wants to upload to cloud, message digest of that file is created and stored in local database with upload details (fig. 3).Then the check for available cloud is done using Byzantine fault-tolerant replication protocol. The Byzantine protocols need a set of storage clouds (n), n = 3f +1, and maximum number of clouds which could be faulty is f. Each file is encrypted and secrete is generated, with the help of Shamir's Secrete sharing scheme n secret parts are generated all parts are stored at different places that is clouds[4].

Message Digest concept MD5 is used for ensuring integrity of data at the time of download phase by comparing MD5 of original file, stored at the time of upload and MD5 generated at the time of download. Data from different cloud can be retrieved only by applying reconstruction algorithm on few (threshold based) or all of the secrete shares from those different clouds. This strongest encryption mechanism is put forward by Adi Shamir[11], based on the idea that two points are sufficient to depict line uniquely, three points to define parabola so on. Based on this at least k points are required to reconstruct a polynomial of degree k-1. This is strongest security scheme, as does not give any knowledge about original data even to the cloud service provider.

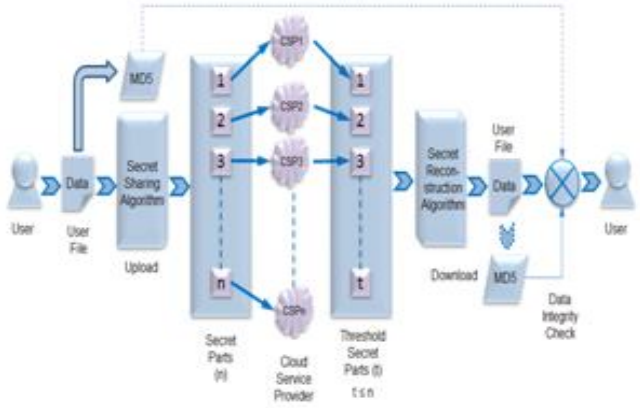

Fig.3 Process of Secure Data Storage &Retrieval using Secret Sharing in Multi-cloud

A. Advantages

A. Data Integrity: One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Use of Byzantine fault-tolerant replication protocol works well for data corruption caused by some components in the cloud. The MD5 File Validation feature provides a technique for users to check that files on the cloud are not corrupted or tampered.

B. Service Availability: Service availability is another major concern in cloud services. The service unavailability can happen due to corruption of data, vender lock-in, possibility of malicious insiders in the single cloud, breakdown of hardware, software or system infrastructure. Replication of data in multiple clouds improves user data availability probability.

C. Confidentiality: This is forbidding the improper disclosure of information. Users important data like passwords, credit card numbers etc. should be kept secret in transit over internet and during storage or retrieval from cloud. This is done using encryption technique named Shamirs secret sharing scheme, which reduces risk of intrusion as hackers need to retrieve all the information from the cloud providers to know the real value of the data in the cloud.

VI. FUTURE WORK

For checking integrity message digest concept is used which is promising but has certain overhead .At the time of each storage and retrieval, message digest has to calculated and checked to validate intactness of data. This should be done by using automated third party auditing mechanism(TPA) as suggested by Cong Wang [7], which is very effective and secure as it does integrity preserving without demanding the local copy of data.

VII. CONCLUSION

A cloud computing is promptly developing area with security as a primary concern[12]. Security is the reason due to which number of the organizations hesitating for going to cloud computing. Cloud clients fear to lose their valuable information due risk of trust on single cloud provider which make move towards use of multi-cloud. Also service availability is area to be concerned in single cloud [14] unlike multi-cloud in which data is replicated to number of clouds. Use of strongest cryptographic algorithm named Shamir's secret sharing algorithm[4], which has number of advantages including security, confidentiality, client-side aggregation etc .Security is harder to compromise as security is maintained even when k or more servers collude, in other words system failing probability is low at worst case also. Data integrity preservation is done through MD5 algorithm. The key conclusion can be made that proposed work provides confidentiality, data integrity, improved availability and capacity to handle multiple requests at a time. The proposed design allows users to store their data securely on cloud with improved availability.

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

[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] C.Cachin, I.Keidarand, A.Shraer, "Trustingthecloud", ACMSIGACT News, 40, 2009, pp.81-86.

[11] Shamir, A. "How to share a secret" Communications of the ACM, 612-613 (1979).

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

[13] 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.

[14] S. Kamara and K Lauter, "Cryptographic cloud storage" , FC'10: Proc. 14th Intl.Conf. on Financial cryptograpy and data security, 2010, pp. 136-149.

[15] 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.

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

[17] 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.