International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Improve Cloud Data Storage Security Using Data Partition Technique

Ms. Yogita Hande[1], Nikhil Pasalkar[2], Mayur Ghatkar[3], Ganesh Narvadkar[4], Prashant Pansare[5]
#Prof., Department of Computer Engineering,
 # Department of Computer Engineering
Sinhgad Institute of Technology and Science, Narhe-411041

Abstract: ***The rapid increment in the popularity of cloud storage services has lead the companies which handle the critical data for their storage needs using cloud services. Examples of critical data includes the dat abases of medical records, historical information about the power system and financial data that can be moved to the cloud. However, yet there are concerns regarding the reliability and security of data stored in the cloud? In this paper we are going to present Multi-Cloud. It is a system that helps to improve the integrity, availability and the confidentiality of the information which is stored in the cloud using the encryption, encoding and replication of the data on diverse clouds that forms a cloud of clouds. This system has been deployed using three clouds and one interpreter.***

General Term: - Cloud Security
Keywords: - Single cloud, Multi cloud, SHA1, AES, SBA.

I. INTRODUCTION

Many organizations have been using cloud computing at a great extent. Many benefits are provided by cloud computing in terms of low cost and accessibility of data.

Maintaining the security in cloud computing is a vital factor in a cloud computing environment because sometimes users store the sensitive information with cloud storage providers but these providers might not be trusted. “single cloud” providers is predicted to be less popular with customers as there are risks of service availability failure along with the possibility of malicious insiders in the single cloud as well. A movement towards “multi-clouds”, or can be said “inter clouds” or “cloud-of-clouds” has evolved recently. It has been found lately that the research into the use of multi-cloud providers for maintaining the security has acquired minimum attention from the research community as compare to the use of single clouds. Thus this work promotes the use of multi- clouds because of its ability to lower the security risks which can affect the cloud computing user.

A. What Is Cloud Computing

Cloud computing depends on sharing the computing resources in spite of having local servers or personal devices to handle applications.

In cloud computing, the word cloud is used as a metaphor for "the Internet". Thus cloud computing means a type of Internet based computing where numerous services like applications, storage and servers are delivered to the computers and the devices of an organization through the Internet.

Cloud computing can be compared to grid computing which is a type of computing where unused processing cycles of all computers in a network are harnesses to solve the intensive problems for any stand-alone machine.

B. Components Of Cloud Computing

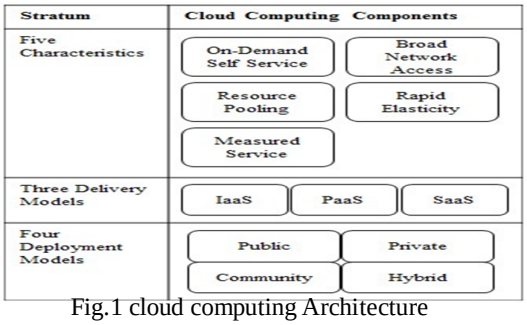

Fig.1 cloud computing Architecture

C. Cloud Computing Environment

In a cloud computing, cloud provides three of its major services Infrastructure as a Services(IaaS), Platform as a Services(PaaS), Software as a Services(SaaS). Let's see the brief discussion of cloud services.

1) Infrastructure as a Service (IAAS):

IaaS covers a number of features from individual servers to private networks, disk drives, long term storage devices and email servers, domain name servers and messaging systems as well. In the very basic cloud-service model physical or virtual machines along with other resources are provided by the IaaS providers to the computers. Sometimes additional resources like images in the virtual machine image library, raw (block) and load balancers, firewalls, file-based storage, IP addresses, virtual local area networks (VLANs), software bundles are offered by the IaaS clouds.

Amazon Cloud Formation, Amazon EC2 are the best examples of IaaS providers

2) Platform as a Service (PAAS):

PaaS enables developers to develop their own applications on top of the platform. This is the reason why it is more extensible than SaaS at the expense of customer-ready features. Wherever the build-in capabilities are less complete, this trade-off extends to security features and capabilities but there is more flexibility to layer on additional security. In the PaaS model, a computing platform such as an operating system, execution environment of a programming language, database servers and the web server are delivered by the cloud providers.

Examples: Cloud Foundry, AWS Elastic Beanstalk, Force.com, Heroku and OrangeScape.

*3) Software as a Service (SAAS)***:**

In the SaaS model, cloud providers install the application software in the cloud and operate it and cloud users access this software from cloud clients. The cloud users don't manage the cloud infrastructure and platform the application is running on. Thus there is no need to install and run the application on the cloud user's own computers simplifying maintenance and support. This is basically end user applications which are delivered on demand over a network based on a pay per use. The installation of the client is not required by the software. It just needs a browser and the network connectivity. Microsoft Office 365 is an example of SaaS. Until it get launched, if a user required says Word, they might have to purchase it, install it and backup files. With Office365 Word can be acquired for small monthly fees without client installation. The files are automatically backed up, software upgrades are automatically received and the software can be accessed from anywhere. If the Word is not required anymore, you can stop paying the monthly fee. It is as simple as that.

Examples: Google apps, MicrosoftOffice365, Onlive, GT Nexus, Marketo, and TradeCard

II. 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 [4]. 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. 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.

Cachin [5] presented a design for intercloud storage named ICStore in 2010.

ICstore is client centric distributed protocol which can handle data integrity issue but has not well performance in case of service availability and data intrusion. It is also happened with encrypted cloud VPN [3].

A. Security Issue In A Single Cloud

Now cloud computing is achieving height of popularity, so cloud related security issues introduced through this new model. The efficiency and effectiveness of traditional security system are being reconsidered as the properties of this changing deployment model can differ highly from those of older architectures. The security of cloud computing services is a argumentative issue that may be delaying its adoption. Private Cloud equipment has a physical control is more secure than having the equipment off site and under someone’s other control.

The ability to visually inspect the data links and access ports with physical control is essential in order to confirm data links are not compromised. Topics barring the acceptance of cloud computing are late in remain part to the public and private sectors' unease neighboring the external management of security based services is the very humor of cloud computing based

services, public or private, that build up external management of given services. This delivers great incentive to cloud computing service providers for strong management of secure services to prioritize building and maintaining. Security issues have been categorized into data segregation, sensitive data access, bug exploitation, privacy, recovery, malicious insiders, accountability, account control, management console security, and multi tenancy issues.

Answers to various cloud security issues vary, from particularly public key infrastructure (PKI) under cryptography, to use of number of cloud providers, standardization of APIs, and developing virtual machine support and legal support. Cloud computing provides lots of benefits, but vulnerable threats also it has .With increasing use of cloud computing, it is more likely that more criminals will shot to search new ways to exploit system's vulnerabilities. There are thousands underlying challenges and risks that increase the threat of data being compromised in cloud computing. To help mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data; establishes trusted foundation to secure the platform and infrastructure; and builds higher assurance into auditing with strengthen compliance. there are Security concerns must be supported in order to create trust in cloud computing technology.

To overcome disadvantages of Single-Cloud System, DepSky architecture is already exists. Now we see DepSky architecture.

B. Dep-Sky Architecture

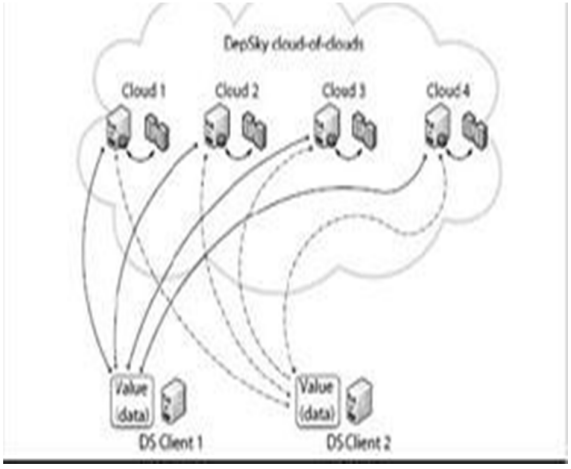

Fig.2 Dep-Sky System Architecture

1) Dep-sky system model:

The DepSky system model assembling with three parts: one reader, one writers, and four cloud storage providers, where client's task are provided readers and writers. Readers can fail number of times (for example, they can fail from time to time, they can fail by crashing, and then show any behavior) whereas, writers only fail only if system crashing.

2) Disadvantages:

First, a data unit of size S consumes n * s storage capacity of the system and costs on average n times more than if it was stored in a single cloud.

Second, it stores the data in clear text, so it does not give confidentiality guarantees.

III. IMPLEMENTATION DETAILS

Objective of our work is to make the ensure that data is in secure and stable form. We are using Multi-Cloud system in our work which contains three storage clouds. It increases the system availability as data is not relayed on a single cloud, also provides data integrity. The Multi-Cloud system also reduces cost of than using single cloud, which is a significant advantage. Our proposed system is used SBA(Seed Block Algorithm) [6] for creating a single cloud backup to Multi-Cloud to provide ensuring of data although data is loss. To make a shift towards more secure cloud computing, we are using multi-cloud computing instead of single cloud computing.

A. Proposed System

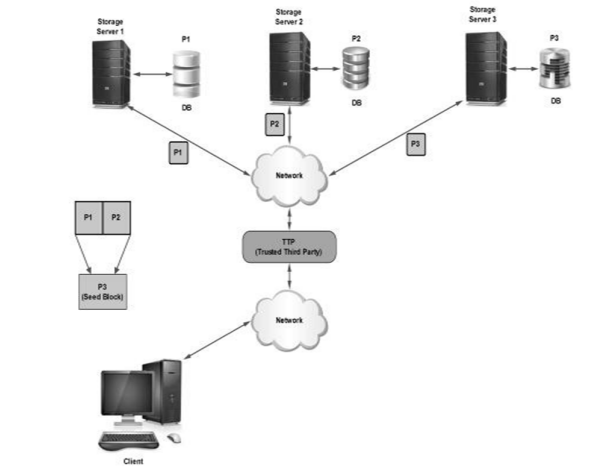

Fig.3 Proposed System Architecture

1) Multi-cloud system model:

Our proposed system model contains three Module: client, TTP and three cloud storage system, where client performs upload and download operation on cloud storage. TTP is mediator between client and cloud storage where it performs backup of a data, encryption of data using AES technic [7] and creating its partition using file partitioning and maintain its hash value using SHA1 algorithm.

A. Seed Block Algorithm

This algorithm points on simplicity of the back-up and recovery process. It normally uses the concept of Exclusive–OR (XOR) operation of the computing world.

For ex: -Suppose there are two data files: A and B. When with XOR of A and B it produced X i.e.

X =A XOR B. If suppose A data file get destroyed and we want our A data file back then we are able to get data file A back, then it is very simple to get back it with the help of B and X data file .i.e. A =X XOR B. Similarly, the Seed Block Algorithm works to provide the simple recovery and Back-up process. Its architecture is consists of the Main Cloud and its clients and the Remote Server. Here, first we set a cloud with a random number and unique client id for very client. Second, whenever the client id is being register in the main cloud; then client id and random number is getting EXORed ( ) with each other to generate seed block for the particular client. The generated seed block corresponds to each client is stored at remote server. Fig 3 shows architecture of seed block algorithm.

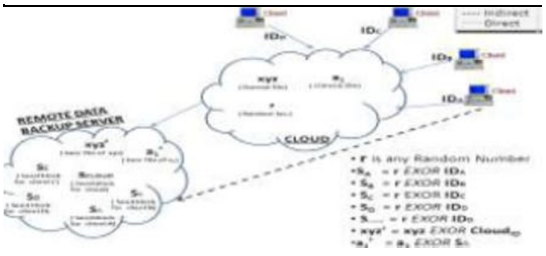

Fig.4 Seed Block Algorithm Architecture

IV. FUTURE WORK

For future work, we aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity.

V. CONCLUSION

Here, we studied what is cloud computing, components of cloud computing, security issues related to single cloud, existing system to overcome disadvantages of single cloud and also try to solve disadvantages of previous system to increase efficiency and security of cloud storage system.

REFERENCES

[1] ”What is cloud computing?” http://www.webopedia.com/TERM/C/cloud_computin g.html
[2] International Journal of Advanced Research in Computer Science and Software Engineering,“Cloud Computing:Service models, Types, Database and issues” by Rahul Bhoyar and Prof. Nitin Chopde, In March 2013
[3] 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.
[4] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6th Conf. On Computer systems, 2011, pp. 31-46
[5] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.
[6] A 2013 International Conference on Communication Systems and Network Technologies, “Seed Block Algorithm: A Remote Smart Data Back- up Technique for Cloud Computing” by Ms. Kruti Sharma.
[7] International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 4 (2013) ISSN 2320-401X; EISSN 2320-4028 ,”A Review of Cryptography Techniques and Implementation of AES for Images” by Mamta. Juneja, and Parvinder S. Sandhu
[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.