Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Improving Security in Cloud Computing Using Secret Sharing Algorithm

Ms. Rupali N. Mahind[1] and Ms. Pooja S. Lokare [2]
[1,2]*Department of Computer Science & Engg.Karad, Satara, India*

Abstract—Basically cloud computing provides a scalable service to easily consumed over the internet as needed. Cloud computing have some benefits in terms of self service provisioning, application programming Interface, Billing & metering of service usage in a pay as you go model. But security and privacy are primary obstacles of cloud. Since cloud computing share distributed resources via network in open environment, thus it makes security problems. The security service includes authentication, encryption, decryption and compression are provide in cloud computing system. Cloud computing promises to cut operational & capital costs focus on strategic projects instead of keeping the data center running. This paper is an attempt to crucial security threats with respect to single cloud and multi cloud .Also focus on the available security measures.

Keywords — Cloud computing, Multicloud , DepSky System ,Secret Sharing algorithm, Message Digest(MD5), Data Integrity

I. INTRODUCTION

Now, days the uses of cloud computing in the organization has increased rapidly .Cloud provider should address privacy and security issues as a matter of high and vital priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the opportunity that there are malicious insiders in the single cloud. In current years, there has been a move towards "multiclouds", "intercloud" or "cloud-of-clouds".[2] As data and information will be shared with a third party, cloud computing users want to keep away from an untrusted cloud provider. Defending private and significant information, such as customer details and a patient's medical records from attackers or malicious behaviors is of serious importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is surveyed. [2]

II. BACKGROUND

In cloud computing allows you to access application that actually located other than your computer or resides on internet connected devices.[1] When you brought Microsoft word & installed it on your computer using CD/DVD. Every time whenever Microsoft issued a new service pack, you have to go around and install that pack or had to set up your software distribution server to distribute it. It license cost also measurable, probably use of word once in month. In cloud computing another company host your application i.e. they handle the costs of servers, they manage the software update & giving access to you depending on your demand because of this you pay less for service.

A. Cloud computing components

Basic characteristics

1) **Elasticity & scalability** – cloud consumer decide how much of any resource they utilize at any time, allocation is driven by immediate demand not need to maintain capacity for peak demand . scalability is that an application can scale when additional users are added and when application requirements change.

2) **On demand Self service** – customers can easily get cloud services without any lengthy process. The customer simply request an amount of computing ,storage ,software ,process or other Resources from service providers. While on demand self provisioning capabilities of cloud service eliminates many time delay.

3) **API** –Interface s provide the instruction on how two applications or data source can communicate with each other.

4) **Flexible Price**- Provides typical charge calculates according to your usage of service. You can pay as you go.

5) **Network Access** – The ability to work with cloud Rs from any point with internet access, cloud service consumer are not dependent on being in corporate head quarter or data center.

6) **Location Independent Rs pool** – Compute and storage Rs may be located anywhere i.e. network accessible, Rs pool enable redundancy and reduce the risk of single point of failure.

B. Delivery Models

1) **Infrastructure as a service (Iaas)** is delivery of computer h/w as a service like servers, networking technology , storage, data centre. This also delivery of OS & virtualization technology to manage Resources .It gives resources on rents instead of buying & installing.Iaas provides low price , Aggregation of resources ,Speed to deployment ,Security .Eg. Amazon Elastic Compute cloud (Amazon EC2) provides web interface to access virtual m/c

2) **Software as a service (Saas)** -provides application or piece of software from service provider. This having some components like
Multi tenancy
Metadata
Infrastructure
Database
Logic
User interface
eg. Salesforce.com

3) **Platform as a service (Paas)** (Also known as cloudware) - Allows the clients to access computing platform over a cloud computing solution .This supplies all resources required to build applications & services from internet without download. Paas includes application design, development, testing, deployment & hosting.

Types of Paas

1. Add on development facilities - allows existing Saas appl to be customize. Paas developers & users are requied to purchase subscriptions to the add- on Saas appl.
2. Standalone env - not include licensing, technical or financial dependencies on Saas.
3. Application delivery-only envy

Support hosting level services like security, on demand scalability not includes development, debugging, testing

III. SECURITY ISSUES

As a part of this paper classify a cloud computing security related issues into following categories.

Table 1. Security Issues

NO.	CATEGORY	ISSUES
C1	Security Standards	-Lack of security standards -Compliance risks -Lack of auditing -Lack of legal aspects (Service level agreement) Trust
C2	Network	-Proper installation of network firewalls -Network security configurations -Internet protocol vulnerabilities -Internet Dependence
C3	Access Control	-Account and service hijacking -Malicious insiders -Authentication mechanism -Privileged user access -Browser Security
C4	Cloud Infrastructure	-Insecure interface of API Quality of service -Sharing technical flaws -Reliability of Suppliers -Security Misconfiguration -Multi-tenancy -Server Location and Backup
C5	Data	-Data redundancy -Data loss and leakage -Data location -Data recovery -Data privacy -Data protection -Data availability

IV. IMPLEMENTATION

The aim of our project is to give guarantee that data is secure when migrating from single cloud to multi cloud. In our project we are using DepSky System as well as secret sharing algorithm .To increase the system availability uses concept of multi cloud by using DepSky system and to provide security to data uses concept of Shamir's secret sharing algorithm.

A. DepSky System-

Bessani et al. [3] present a virtual storage cloud system called DepSky on which consist of a combination of different storage clouds to build multi cloud architecture. This system provides availability & confidentiality of data in storage system.

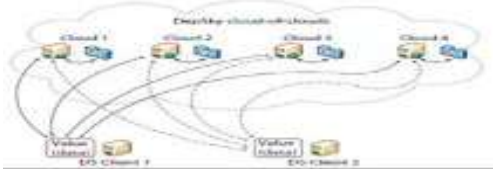

Figure 1. DepSky Architecture

Figure 1 shows four clouds and each cloud having its own particular interface. These four clouds are storage clouds without capacity of executing user's code. The DepSky algorithm exist in the client machine as software library. This library allows to different cloud interface provides and data format is accepted from each cloud.

B. Data Model

This model consist of three abstraction levels .The first level of abstraction is conceptual data unit having basic storage object with which corresponding algorithm works. Each data unit has unique name ,version number(to support updates on the object), verification data(usually a cryptographic hash of the data) and actual data which stored on the data unit object. The second level is generic data unit or container, contains two types of files:1. metadata file- having version number and the verification data and other information related to application. 2. The files that store the data. Third abstraction level is Data unit Implementation i.e. container translated into specific constructions supported by each cloud provider.

C. System Model

It has readers, writers and cloud storage providers. Readers and writers are nothing but the client. As shown in Figure 1,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 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 [4]. All writers of a data unit have common private key used to sign some of the data written on the data unit , while readers have access to the corresponding public key to verify these signatures. This public key can be made available to the readers through the storage clouds themselves. We also assume that passive storage entity that supports some operations like: list (lists the files of a container in the cloud), get (reads a file), create (creates a container), put (writes or modifies a file in a container) and remove (deletes a file)[5].

D. Security using Secret Sharing Algorithm

we do not trust on single clouds, assume they can fail in a Byzantine way data stored can be deleted, corrupted, created or leaked to unauthorized parties. This will be happen by both ways malicious attacks/intrusions on a cloud provider and arbitrary data corruption (e.g., due to accidental events). The protocols require a set of storage clouds (n), $n = 3 f + 1$, f is max number of clouds which can be faulty. Additionally, the quorums used in the protocols are composed by any subset of $(n - f)$ storage clouds. This is the minimum number of replicas to tolerate Byzantine servers in asynchronous storage systems[2].

If we simply replicate the data on n clouds, the costs of storing data using DepSky would increase by a factor of n. To avoid this, we compose the secret sharing scheme used on the protocol with an information optimal erasure code algorithm for reducing the size of each share by factor of n. In our proposed system we have to give assurance about to prevent security risk. DepSky model and secret sharing algorithm is used to reduce risk of data intrusion and loss of service availability in cloud. File can be upload or download 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. The data is encrypted with a random secret key, the encrypted data is encoded, the key is divided using secret sharing and each server receives a block of the encrypted data and a share of the key. In the Shamir's Secrete sharing scheme, secrete is divided into parts and then all parts are stored at different clouds. So to reconstruct original secrete, one has to acquire all or some parts of the secrete from those different clouds [6].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.

For this use Message Digest Concept. Message Digest concept MD5 is used for ensuring integrity of data at the time of upload phase as shown in figure 2. 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.

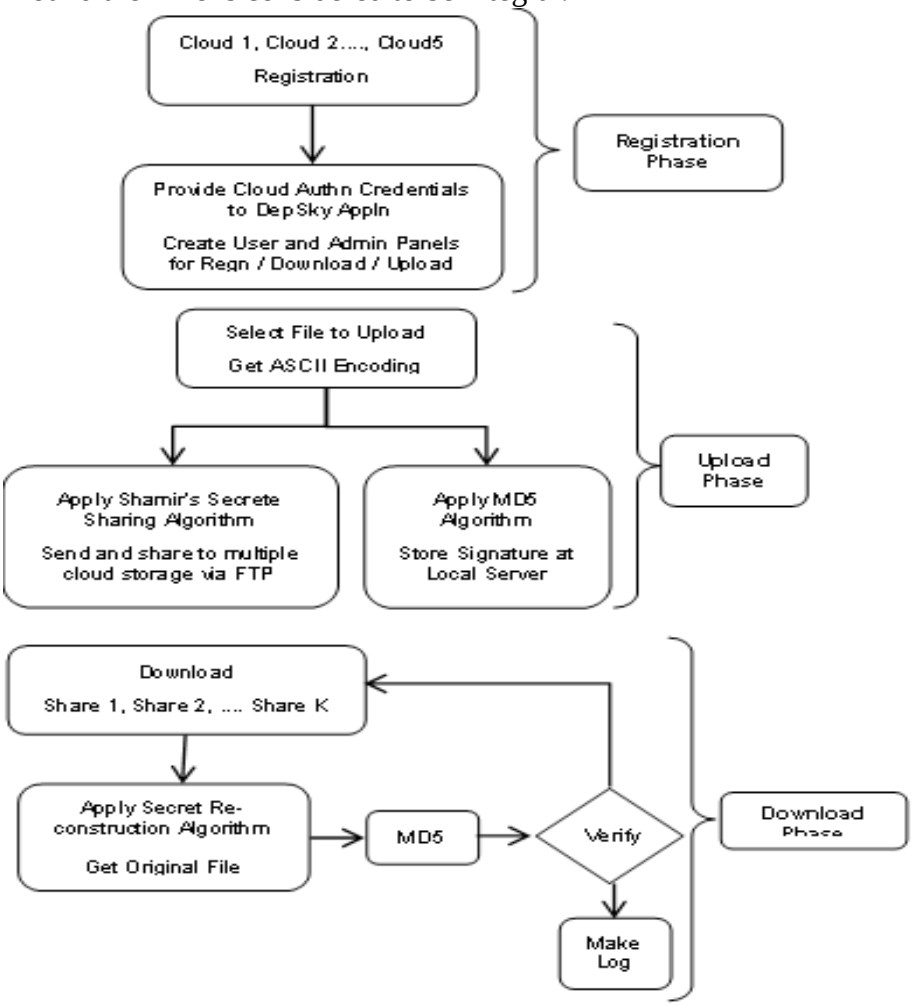

Figure 2.Data Flow

Shamir's secret sharing scheme is a threshold scheme based on polynomial function technique. It allows a Server S to distribute a secret value s to n clouds, such that some of parts required to reconstruct the secret. The protocol information theoretically secure, i.e., any fewer than t(threshold) clouds cannot gain any information about the secret by themselves.

V. CONCLUSION

Cloud computing has been showing its impact on the industry for the past few years and it has a revolutionary change giving new directions to how information technology resources can be best utilized and by reducing the cost and complexity for customers.

In this paper, we have given a brief analysis of various security concerns of cloud computing. We will try to come forward with more innovative ideas and security measure in future. In this paper, we have made an attempt to analyze the various security concerns of cloud computing and has provided some security measures. Even though Cloud Computing offers a wide range of benefits and newer services, people express different opinions about the security aspects of it. Because of these security concerns, it is still not gaining its full momentum. Most of the organizations are stepping back as they don't want to take the security risk. It is essential to have more standard security measures for cloud computing in order to gain complete acceptance from all levels of organizations.

REFERENCES

[1] NIST), http://www.nist.gov/itl/cloud/
[2] 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
[3] 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
[4] Swapnila S Mirajkar, IISantoshkumar Biradar ," Using Secret Sharing Algorithm for Improving Security in Cloud Computing" International Journal of Advanced Research in Computer Science & Technology (IJARCST)2014
[5] Dhulipala. SivaKumar B.Narsimha Dr. N. SubashChandra G.CharlesBabu SP. Santhosh ," Using Secret Sharing Algorithm for Improving Security in Cloud Computing" International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)
[6] Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), 2010, pp. 17-23.

