Enhancing Cloud Computing Security by using Multi-Cloud Strategy*

Shaikh Sadaf Ahmed (Author)

Department of Computer Engineering, Pillai Institute of Information Technology, New Panvel, University of Mumbai, Maharashtra, India

E-mail address:[nashrashaikh20@gmail.com]

ABSTRACT

The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud.

Single cloud provider is less popular due to service availability failure, data integrity or malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has emerged recently.

This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user. Multi-cloud strategy is the concomitant use of two or more cloud services to minimize the data loss due to failure in cloud. Multi-cloud environment controls the several clouds and avoids the dependency on any one individual cloud.

This paper introduces the DepSky System model which is the dependable and secure storage system that gives the benefits of the cloud computing by using the combination of the diverse commercial clouds to build the Multi-cloud. DepSky system addresses the four important limitations of cloud computing i.e. Loss of availability, Loss of corruption of Data, Loss of privacy and Vendor-Lock-in.Main purpose of moving to Multi-clouds is to improve what was offered in single clouds by distributing reliability, trust, and security among multiple cloud providers.

Index Terms:

Cloud computing, single cloud, multi-clouds, cloud storage, data integrity, data intrusion, service availability.

I. INTRODUCTION

The use of cloud computing has increased rapidly in many organizations. Small and medium companies use cloud computing services, because these services provide fast access to their applications and reduce their infrastructure costs. Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multiclouds", "intercloud" or "cloud-of-clouds".

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, from attackers or malicious insiders is of critical 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.

II. OBJECTIVE

As we know the use of cloud computing has increased in many organizations. Most of the companies use the cloud computing services because of its features. Dealing with the single cloud provider is less popular; hence use of Multi-cloud is more dominant (powerful).

III. BACKGROUND

1. Cloud Computing.

1.1 Cloud Computing Components.

The cloud computing Model consists of five charactestics, three delivery models and four deployments model.

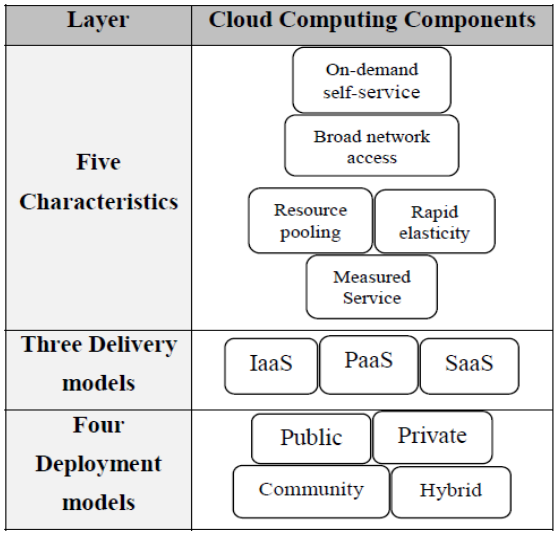

Fig 1: Cloud Environnement Architecture.

Characteristics of Cloud computing [5] [6]

- **On-demand self service**

Cloud computing provides on demand service means users can access the service of cloud whenever they need it. In cloud computing user will have to pay only for the services that they are using.

- **Broad network access**

With the help of smart phones, tablet user can access their data from the clouds anytime and from anywhere this mobility is particularly attractive for businesses so that during business hours or on off-times, employees can stay connected with their work and customers whether they are on the road or in the office.

- **Resource pooling [4]**

The cloud enables your employees to enter and use data within the business management software hosted in the cloud at the same time, from any location, and at any time. This is an attractive feature for multiple business offices and field service or sales teams that are usually outside the office.

- **Rapid elasticity**

If anything happens, the cloud is flexible and scalable to suit your immediate business needs. You can quickly and easily add or remove users, software features, and other resources.

- **Measured service**

As we know in cloud, you only pay for what you use. You and your cloud provider can measure storage levels, processing, bandwidth, and the number of user accounts and you are billed appropriately. The amount of resources that you may use can be monitored and controlled from both your side and your cloud provider's side which provides transparency.

Delivery models are:

- **Infrastructure as a service (IaaS)**

In IaaS the user can benefit from networking infrastructure facilities, data storage and computing services. For example Amazon Web service.

- **Platform as a service (PaaS)**

In PaaS, the user runs custom applications using the service provider's resources. For example GoogleApps.

- **Software as a Service (SaaS)**

Running software on the provider's infrastructure and providing licensed applications to users to use services is known as SaaS. For example Salesforce.com CRM application.

Deployments model:

- **Public clouds:** A cloud environment that is accessible for multi-tenants and is available to the public is called a public cloud.
- **Private Clouds:** A private cloud is available for a particular group.
- **Community cloud:** Community cloud is modified for a particular group of customers
- **Hybrid cloud:** Hybrid cloud is a composition of two or more clouds (private, community or public)

1.2 Cloud Service provider

Cloud Service Provider offers the services i.e Iaas, SaaS and PaaS to the organizations or individuals. The service providers take care of the customer's needs.

Cloud service providers should ensure the security of their customers' data and should be responsible if any security risk affects their customers 'service infrastructure. A cloud provider offers many services that can benefit its customers, such as fast access to their data from any location, scalability, pay-for-use, data storage, data recovery, protection against hackers, on-demand security controls, and use of the network and infrastructure facilities.

2. Security Risks in Cloud Computing

As the cloud services have been built over the Internet, any issue that is related to internet security will also affect cloud services. The technology used in the cloud is similar to the technology used in the Internet. Encryption techniques and secure protocols are not sufficient to protect data transmission in the cloud. Data intrusion of the cloud through the Internet by hackers and cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients.

Three security factors that affect the single cloud:

2.1 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. One solution is to use a Byzantine fault-tolerant replication protocol within the cloud. This solution can avoid data corruption caused by some components in the cloud, but a Byzantine fault-tolerant protocol across multiple clouds from different providers is a beneficial solution.

2.2 Data Intrusion:

If someone gains access to someone's account password, then they will be able to access all the information inside the account. Thus the stolen password allows the hacker to erase as well as modify all the information inside the account. This type of security risk is known as data intrusion attack.

2.3 Service Availability:

Another major concern in cloud services is service availability; it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy which results in service unavailability. Therefore one solution to this risk is to use multiple clouds and store the data on multiple clouds instead of one cloud. Thus even if the one cloud service is fail, the uer still be able to retrieve their data from other clouds.

IV. RESEARCH METHODOLOGY

Multi-clouds Computing security

[7]

Multi-Clouds: Preliminary

The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" These terms suggest that cloud computing should not end with a single cloud. Using their illustration, a cloudy sky incorporates different colors and shapes of clouds which leads to different implementations and administrative domains. Multi-cloud environment controls several clouds and avoids dependency on any one individual cloud.

Introduction to Byzantine Protocol [3]

In cloud computing, any faults in software or hardware are known as Byzantine faults that usually relate to inappropriate behavior and intrusion tolerance. In addition, it also includes arbitrary and crash faults. BFT protocols are not suitable for single clouds. Limitations of BFT for the inner-cloud is that BFT requires a high level of failure independence, as do all fault-tolerant protocols. If Byzantine failure occurs to a particular node in the cloud, it is reasonable to have a different operating system, different implementation, and different hardware to ensure such failure does not spread to other nodes in the same cloud. In addition, if an attack happens to a particular cloud, this may allow the attacker to hijack the particular inner-cloud infrastructure.

DEPSKY System: Multi-Clouds Model

[1]

DEPSKY, a dependable and secure storage system that leverages the benefits of cloud computing by using a combination of diverse commercial clouds to build a cloud-of-clouds.

DEPSKY addresses four important limitations of cloud computing for data storage.

- **Loss of availability**

DEPSKY deals with this problem by storing the data on a multiple clouds, thus even if one cloud is down or service is unavailable, data can be retrieved from the other clouds.

- **Loss or corruption of data**

DEPSKY deals with this problem using Byzantine fault-tolerant replication to store data on several cloud services, allowing data to be retrieved correctly even if some of the clouds corrupt or lose data.

- **Loss of privacy**

The cloud provider has access to both the data stored in the cloud and metadata like access patterns. The provider may be trustworthy, but malicious insiders are a wide-spread security problem. This is an especial concern in applications that involve keeping private data. An obvious solution is the customer encrypting the data before storing it, but if the data is accessed by distributed applications this involves running protocols for key distribution. DEPSKY employs a secret sharing scheme and erasure codes to avoid storing clear data in the clouds and to improve the storage efficiency, amortizing the replication factor on the cost of the solution.

- **Vendor-lock-in**

There is currently some concern that a few cloud computing providers become dominant, the so called vendor lock-in issue. Even moving from one provider to another one may be expensive because the cost of cloud usage has a component proportional to the amount of data that is read and written. DEPSKY addresses this issue in two ways. First, it does not depend on a single cloud provider, but on a few, so data access can be balanced among the providers considering their practices (e.g., what they charge). Second, DEPSKY uses erasure codes to store only a fraction (typically half) of the total amount of data in each cloud.

DEPSKY Architecture

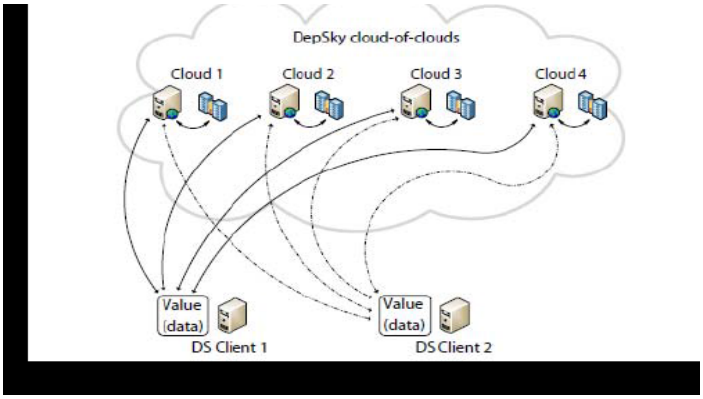

Fig 2: DepSky Architecture

Fig 2 presents the architecture of DEPSKY. The DEPSKY algorithms are implemented as a software library in the clients. This library offers an object store interface , similar to what is used by parallel file systems, allowing reads and writes in the back-end (in this case, the untrusted clouds).

DEPSKY Data model. [1]

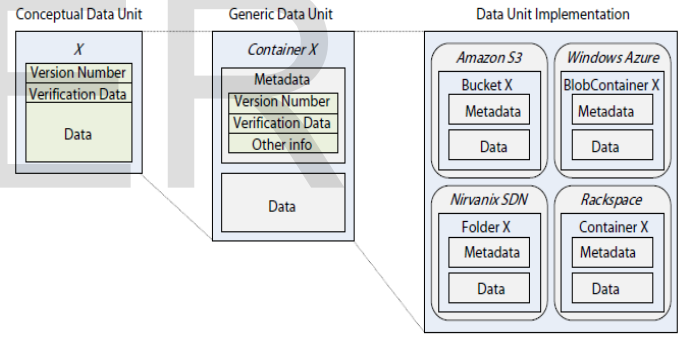

Fig 3. DEPSKY data unit and the 3 abstraction levels.

Fig 3 presents the DEPSKY data model with its three abstraction levels. In the first (left), there is the conceptual data unit, which corresponds to the basic storage object with which the algorithms work. A data unit has a unique name (X in the figure), 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. In the second level (middle), the conceptual data unit is implemented as a generic data unit in an abstract storage cloud. Each generic data unit, or container, contains two types of files: a signed metadata file and the files that store the data. Metadata files contain the version number and the verification data, together with other

informations that applications may demand. Notice that a data unit (conceptual or generic) can store several versions of the data, i.e., the container can contain several data files. The name of the metadata file is simply metadata, while the data files are called value<Version>, where <Version> is the version number of the data (e.g., value1, value2, etc.). Finally, in the third level (right) there is the data unit implementation, i.e., the container translated into the specific constructions supported by each cloud provider (Bucket, Folder, etc.).

The data stored on a data unit can have arbitrary size, and this size can be different for different versions. Each data unit object supports the usual object store operations: creation (create the container and the metadata file with version 0), destruction (delete or remove access to the data unit), write and read.

DEPSKY System model [1]

The DepSky system model contains three parts: readers, writers, and four cloud storage providers.

Readers and writers: Readers can fail arbitrarily, i.e., they can crash, fail intermittently and present any behavior. Writers, on the other hand, are only assumed to fail by crashing. We do not consider that writers can fail arbitrarily because, even if the protocol tolerated inconsistent writes in the replicas, faulty writers would still be able to write wrong values in data units, effectively corrupting the state of the application that uses DEPSKY. Moreover, the protocols that tolerate malicious writers are much more complex with active servers verifying the consistency of writer messages, which cannot be implemented on general storage clouds

All writers of a data unit du share a common private key K_{rw}^{du} used to sign some of the data written on the data unit (function sign(DATA; K_{rw}^{du})), while readers of du have access to the corresponding public key K_{uw}^{du} to verify these signatures (function verify (DATA; K_{uw}^{du})). Moreover, we assume also the existence of a collision-resistant cryptographic hash function H.

Cloud storage providers: Each cloud is modeled as a passive storage entity that supports five operations: 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). By passive storage entity, we mean that no protocol code other than what is needed to support the aforementioned operations is executed. We assume that access control is provided by the system in order to ensure that readers are only allowed to invoke the list and get operations.

V. FINDINGS / ANALYSIS OF MULTI-CLOUD RESEARCH

Main purpose of moving to interclouds is to improve what was offered in single clouds by distributing reliability, trust, and security among multiple cloud providers. In addition, reliable distributed storage which utilizes a subset of BFT techniques to be used in multi-clouds. [2]

RACS (Redundant Array of Cloud Storage) for instance, utilizes RAID-like techniques that are normally used by disks and file systems, but for multiple cloud storage. To avoid "vender lock-in", distributing a user's data among multiple clouds is a helpful solution. Therefore, the storage load will be spread among several providers as a result of the RACS proxy.

HAIL (High Availability and Integrity Layer) is another protocol that controls multiple clouds. HAIL is a distributed cryptographic system that permits a set of servers to ensure that the client's stored data is retrievable and integral. HAIL provides a software layer to address availability and integrity of the stored data in an intercloud.

A virtual storage cloud system called DepSky consisting of a combination of different clouds to build a cloudof- clouds. some limitations of the HAIL protocol and RACS system when compared with DepSky are HAIL does not guarantee data confidentiality, it needs code execution in their servers, and it does not deal with multiple versions of data. None of these limitations are found in DepSky whereas the RACS system differs from the DepSky system in that it deals with "economic failures" and vendor lock-in and does not address the issue of cloud storage security problems.

Current Solutions of Security Risks

In order to reduce the risk in cloud storage, customers can use cryptographic methods to protect the stored data in the cloud. Loss of availability of service is one of the main limitations in cloud computing and it has been addressed by storing the data on several clouds. The loss of customer data has caused many problems for many users, to solve this use of Byzantine fault-tolerant replication protocol is beneficial solution, so if one of the cloud providers is damaged, they are still able to retrieve data correctly. Data encryption is considered the solution by to address the problem of the loss of privacy. As the data will be accessed by distributed applications, the DepSky system stores the cryptographic keys in the cloud by using the secret sharing algorithm to hide the value of the keys from a malicious insider. In the DepSky system, data is replicated in four commercial storage clouds (Amazon S3,Windows Azure, Nirvanix and Rackspace); it is not relayed on a single cloud, therefore, this avoids the problem of the dominant cloud causing the so-called vendor lock-in issue.

Suggestions/ Future Work:

For the future work, the main aim is to provide a framework to supply a secure cloud database that will guarantee to prevent the security risk. This framework should 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. For Data intrusion and Data integrity, assume we want to distribute the data into three different cloud providers and we apply the secret sharing algorithm on that stored data, so for this an intruder needs to retrieve at least three values to be able to find out the real values that we want to hide from the intruder. In other words, hackers need to retrieve all the information from the cloud providers to know the real value of the data in the cloud. Hence, replicating data into multi-clouds by using a multi-share technique may reduce the risk of data intrusion and increase data integrity. Regarding the service availability risk or loss of data, if we replicate the data into multiple cloud providers then the data loss risk will be reduced. Hence if one cloud provider fails we can still be able to access our data from the other cloud provider.

VI. ACKNOWLEDGEMENT

I thank the Lord Almighty for his grace and blessings which help me to complete this study.

I would like to express my deep sense of gratitude to my guide Prof. Dipti Patil, for her valuable guidance, patience, keen interest and constant encouragement.

My heartfelt gratitude to the H.O.D of COMPUTER ENGINEERING Department Prof.Varunakshi Bhojane and M.E coordinator Prof. Sharvari Govilkar who have always been there to help and give their time and advice in spite of their busy schedule.

I would like to thank our principal Dr. R.I.K. Moorthy and my college Pillai Institute of Information Technology, New Panvel.

I would like to thank my colleague Ms. Shweta Pathak for her valuable guidance and support.

I thank all the Professors who have validated my tool and given their valuable opinion.

VII. CONCLUSION

It is clear that the use of cloud computing has increased rapidly but the cloud computing security is still major issue in cloud computing environment. Customers do not want to lose their private information as malicious insiders in the cloud. There are various security risk in cloud computing i.e. data integrity, service availability and data intrusion.

The purpose of research on single clouds and multi clouds is to address the security risk and solutions. Much Research has been done on single clouds and cloud storage whereas the multi cloud received less attention in the security. Migration to multi cloud addresses the security risk that affects the cloud computing users.

VIII. REFERENCES

[1] 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.

[2] 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

[3] 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.

[4] http://en.wikipedia.org/wiki/Cloud_computing

[5] http://www.cloudtweaks.com/2012/09/key-features-of-cloud-computing/

[6] http://erpbloggers.com/2013/07/the-five-essential-characteristics-of-cloud-computing/

[7] http://searchcloudapplications.techtarget.com/definition/multi-cloud-strategy