Providing Security for Multi-Clouds

K . Manoj
PG - Dept. of CSE
Madanapalle Institute of Technology & Science
Madanapalle, Andhra Pradesh, India

M . D . Shaheer Banu
PG - Dept. of CSE
Madanapalle Institute of Technology & Science
Madanapalle, Andhra Pradesh, India

S . Fairoja
PG - Dept. of CSE

Madanapalle, Andhra Pradesh, India

***Abstract*— Cloud computing is computing that involves a large number of computers connected through a communication network such as the Internet. The term "the cloud" is essentially a metaphor for the Internet. As the security in single clouds is becoming a challenge to provide we move on to multi clouds by splitting a single file to multiple files and store them in different servers. We split a single file into small four different files encrypt them and store them in four different servers in order to provide security. When any intruders enter into the server they can't get any access to the files.**

Index Terms—Cloud Computing, Depsky System, Byzantine Protocols, Multi-clouds.

I. INTRODUCTION

The use of cloud computing has increased rapidly in many organizations. Subashini and Kavitha argue that small and medium companies use cloud computing services for various reasons, including 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 "multi clouds", "inter cloud" or "cloud-of-clouds".

II. RELATED WORK

Cloud computing as "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 interaction".

A. Cloud Computing Components

The cloud computing model consists of five characteristics, three delivery models, and four deployment models. The five key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured service. These five characteristics represent the first layer in the cloud environment architecture.

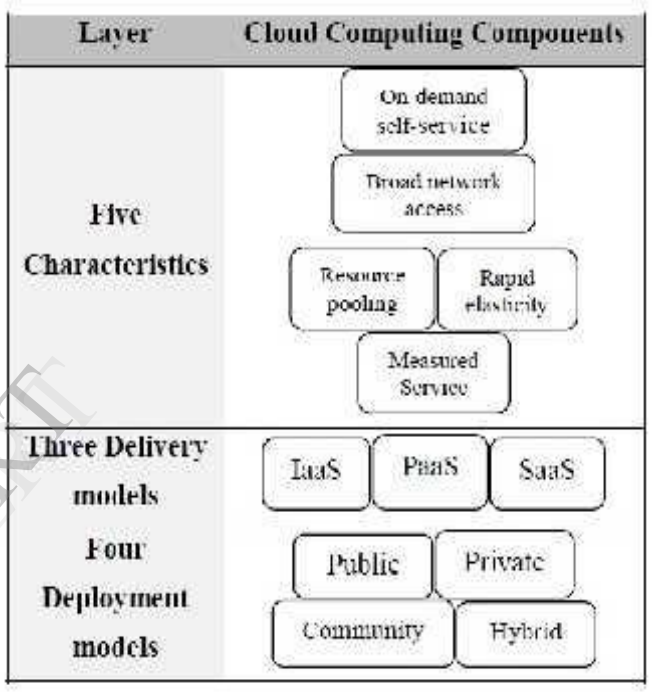

Fig. 1. Architecture Diagram

The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service(PaaS), and software as a service (SaaS). In IaaS, the user can benefit from networking infrastructure facilities, data storage and computing services. In other words, it is the delivery of computer infrastructure as a service. An example of IaaS is the Amazon web service. In PaaS, the user runs custom applications using the service provider's resources. It is the delivery of a computing platform and solution as a service. An example of PaaS is GoogleApps. Running software on the provider's infrastructure and providing licensed applications to users to use services is known as SaaS. An example of SaaS is the Salesforce.com CRM application.This model represents the second layer in the cloud environment architecture. Cloud deployment models include public, private, community, and hybrid clouds. A cloud environment that is accessible for multi-tenants and is available to the public is called a public cloud. A private cloud is available for a particular group, while a community cloud is modified for a specific group of customers. Hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public cloud). This model represents the third layer in the cloud environment architecture.

B. Cloud Service Providers Examples

In the commercial world, various computing needs are provided as a service. The service providers take care of the customer's needs by, for example, maintaining software or purchasing expensive hardware. For instance, the service EC2, created by Amazon, provides customers with scalable servers. As another example, under the CLuE program, NSF joined with Google and IBM to offer academic institutions access to a large-scale distributed infrastructure. There are many features of cloud computing. First, cloud storages, such as Amazon S3, Microsoft Sky Drive, or Nirvanix Cloud NAS, permit consumers to access online data. Second, it provides computation resources for users such as Amazon EC2. Third, Google Apps or versioning repositories for source code are examples of online collaboration tools.

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.

Reliability and availability are other benefits of the public cloud, in addition to low cost. However, there are also concerning issues for public cloud computing, most notably, issues surrounding data integrity and data confidentiality. Any customer will be worried about the security of sensitive information such as medical records or financial information.

III. SECURITY RISKS IN CLOUD COMPUTING

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment. Users of online data sharing or network facilities are aware of the potential loss of privacy. According to a recent IDC survey the top challenge for 74% of CIOs in relation to cloud computing is security. Protecting private and important information such as credit card details or patients' medical records from attackers or malicious insiders is of critical importance. Moving databases to a large data centre involves many security challenges such as virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft. Some fundamental security challenges, which are data storage security, application security, data transmission security, and security related to third-party resources.

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. Examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution server. Another example of breached data occurred in 2009 in Google Docs, which triggered the Electronic Privacy Information Centre for the Federal Trade Commission to open an investigation into Google's Cloud Computing Services. Another example of a risk to data integrity recently occurred in Amazon S3 where users suffered from data corruption.

B. Data Intrusion

According to Garfinkel[19], another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked (see [18] for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

C. Service Availability

Another major concern in cloud services is service availability. Amazon mentions in its licensing agreement that 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. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure.Companies seeking to protect services from such failure need measures such as backups or use of multiple providers . Both Google Mail and Hotmail experienced service downtime recently. If a delay affects payments from users for cloud storage, the users may not be able to access their data. Due to a system administrator error, 45% of stored client data was lost in LinkUp (MediaMax) as a cloud storage provider.

IV. MULTI-CLOUDS COMPUTING SECURITY

The migration of cloud computing from single to multi-clouds to ensure the security of the user's data.

A. Multi-Clouds Preliminary

The term "multi-clouds" is similar to the terms "interclouds" or "cloud-of-clouds" that were introduced by Vukolic. 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. Recent research has focused on the multi-cloud environment [3],[8],[10],[11] which control several clouds and avoids dependency on any one individual cloud.

B. Introduction to Byzantine Protocols

In cloud computing, any faults in software or hardware are known as Byzantine faults that usually relate to inappropriate behaviour and intrusion tolerance. In addition, it also includes arbitrary and crash faults. Much research has been dedicated to Byzantine fault tolerance (BFT) since its first introduction. Although BFT research has received a great deal of attention, it still suffers from the limitations of practical adoption and remains peripheral in distributed systems. The relationship between BFT and cloud computing has been investigated, and many argue that in the last few years, it has been considered one of the major roles of the distributed system agenda. Furthermore, many describe BFT as being of only "purely academic interest" for a cloud service. This lack of interest in BFT is quite different to the level of interest shown in the mechanisms for tolerating crash faults that are used in large-scale systems

C. Depsky System: Multi-clouds Model

This section will explain the recent work that has been done in the area of multi-clouds. Bessani et al. [8] present a virtual storage cloud system called DepSky which consists of a combination of different clouds to build a cloud-of-clouds. The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers, combining Byzantine quorum system protocols, cryptographic secret sharing and erasure codes.

1) Depsky Architecture

The DepSky architecture consists of four clouds and each cloud uses its own particular interface. The DepSky algorithm exists in the clients' machines as a software library to communicate with each cloud. These four clouds are storage clouds, so there are no codes to be executed. The DepSky library permits reading and writing operations with the storage clouds.

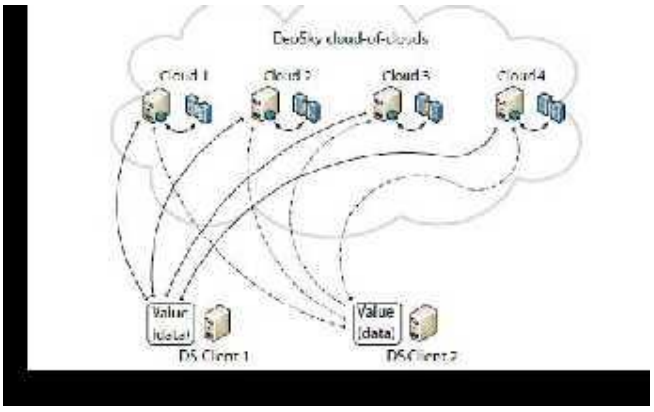

Fig. 2. Depsky Architecture

Depsky Data Model

As the DepSky system deals with different cloud providers, the DepSky library deals with different cloud interface providers and cloud. The DepSky data model consists of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation.

Depsky System Model

The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas, writers only fail by crashing.

V. LIMITATIONS OF CURRENT SOLUTIONS

The problem of the malicious insider in the cloud infrastructure which is the base of cloud computing. IaaS cloud providers provide the users with a set of virtual machines from which the user can benefit by running software on them. The traditional solution to ensure data confidentiality by data encryption is not sufficient due to the fact that the user's data needs to be manipulated in the virtual machines of cloud providers which cannot happen if the data has been encrypted. Administrators manage the infrastructure and as they have remote access to servers, if the administrator is a malicious insider, then he can gain access to the user's data. VanDijk and Juels present some negative aspects of data encryption in cloud computing. In addition, they assume that if the data is processed from different clients, data encryption cannot ensure privacy in the cloud.

VI. CONCLUSION AND 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.

If a file in the server is missing due to intruders or service availability it can be retrieved by creating a cache file in other servers and can be retrieved as a whole file without any lose of data.

REFERENCES

[1] (NIST), http://www.nist.gov/itl/cloud/.

[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[3] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security &Privacy,8(6),2010,pp.24-31

ISSN: 2278-0181

[4] F. Rocha and M. Correia, "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", Proc. 1stIntl. Workshop of Dependability of Clouds, Data Centers and Virtual Computing Environments, 2011, pp. 1-6.

[5] P.A. Loscocco, S.D. Smalley, P.A. Muckelbauer, R.C. Taylor, S.J. Turner and J.F. Farrell, "The inevitability of failure: The flawed assumption of security in modern computing environments", Citeseer, 1998, pp. 303-314.

[6] M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing", HotSec'10: Proc. 5thUSENIX Conf. on Hot topics in security, 2010, pp.1-8.

[7] U. Maheshwari, R. Vingralek and W. Shapiro, "How to build a trusted database system on untrusted storage", OSDI'00: Proc. 4thConf. On Symposium on Operating System Design & Implementation, 2000, p. 10.

[8] F. Schneider and L. Zhou, "Implementing trustworthy services using replicated state machines", IEEE Security and Privacy, 3(5),2010, pp. 151-167.