MULTI CLOUD COMPUTING WITH SECURITY FRAMEWORK

[1]R.Gnanakumari

[1]Assistant Professor/CSE, Department of ECE,

Nehru Institute of Engineering and Technology, Coimbatore, India
mailtokumari81@gmail.com

Abstract—Cloud computing is used by most of the people in recent days. 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 deal with "single cloud". There may be service availability failure and there is possibility of malicious insiders being in the single cloud. A movement towards "multi-clouds" has become popular recently. This paper focus on multi clouds usage and how to use multi cloud environment with a security mechanism. This work aims to promote the use of multi-clouds and to reduce security risks that affect the cloud computing user.

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

1 INTRODUCTION

Cloud computing is a paradigm shift that enables scalable processing and storage over distributed, networked commodity machines. Enterprises that want to reap the benefits of cloud computing must realize that the decision to migrate is neither quick nor easy. The extensibility and flexibility of software architectures and the promise of distributed computing have created a concept known as cloud computing. The cloud shifts the centralized, owned-and-operated computing infrastructure model to a fully distributed decentralized paradigm. To enable the cloud, data centers leverage commodity hardware, virtualization techniques, open frameworks, and ubiquitous network access.

Grid computing was generally used to run a few processor-intensive tasks that would normally be run on a high-performance machine, Cloud computing extends this concept to perform multiple tasks for numerous users in a distributed fashion. The network (intranet or Internet) is employed to interconnect commodity machinery and to deliver services to disparate User.

- Mrs.R.Gnanakumari is working as Assistant Professor in ECE in Nehru Institute of Engineering and Technology, Coimbatore, India.
E-mail: mailtokumari81@mail.com

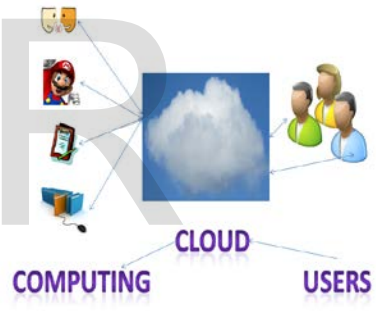

Figure 1.Cloud Architecture

2. CLOUD ARCHITECTURE

The systems architecture(figure1) of the software systems involved in the delivery of cloud computing, typically involves multiple *cloud components* communicating with each other over application programming interfaces, usually web services and 3-tier architecture. This resembles the UNIX philosophy of having multiple programs each doing one thing well and working together over universal interfaces. Complexity is controlled and the resulting systems are more manageable than their monolithic counterparts.

The two most significant components of cloud computing architecture are known as the front end and the back end. The front end is the part seen by the client, i.e. the computer user. This includes the client's network (or computer) and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the 'cloud' itself, comprising various computers, servers and data storage

devices.

2.1 Cloud Computing Types

Public cloud

Public cloud or external cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis.

Hybrid cloud

A hybrid cloud environment consisting of multiple internal and/or external providers "will be typical for most enterprises".

Private cloud

Private cloud and internal cloud are neologisms that some vendors have recently used to describe offerings that emulate cloud computing on private networks. These (typically virtualization automation) products claim to "deliver some benefits of cloud computing without the pitfalls", capitalizing on data security, corporate governance, and reliability concerns.

2.2 Cloud Computing Categories

Infrastructure as a Service (IaaS)

Cloud infrastructure services or "Infrastructure as a Service (IaaS)" delivers computer infrastructure, typically a platform virtualization environment as a service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service.

Examples:- IBM Blue house, VMWare, Amazon EC2, Microsoft Azure Platform, Sun Parascale and more

Benefits to the clients:

- Stop worrying about heavy traffic and bandwidth requirements.
- Pay as you go.
- No need to buy high configuration servers from day one.
- Low maintenance.

Platform as a Service (PaaS)

Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer Force.com, (an outgrowth of Salesforce.com) and GoogleApps are examples of PaaS. Examples:- Middleware, Intergation, Messaging, Information, connectivity etc AWS, IBM Virtual images, Boomi, CastIron, Google Appengine

Software as a Service (SaaS)

In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. The end user is free to

Examples:-Gmail, Google Calendar Payroll, HR, CRM.

3. 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. We will address three security factors that particularly affect single clouds, namely data integrity, data intrusion, and service availability.

3.1 Data Integrity

One of the most important issues related to cloud Security risk is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Recently Red Hat Linux's distribution servers had a problem. 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

3.2 Data Intrusion

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. Furthermore, there is a possibility for the user's email (Amazon user name) to be hacked, 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.

3.3 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. 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. Information privacy is not guaranteed in Amazon S3. use the service from anywhere.

4. Multi-Clouds Computing Security

This section will discuss the migration of cloud computing from single to multi-clouds to ensure the security of the user's data.

4.1 Multi-Clouds: Preliminary

The term "multi-clouds" is similar to the terms "inter clouds" or "cloud-of-clouds" that were introduced by Vukolic. These terms suggest that cloud computing should not end with a single cloud. Recent research has focused on the multi- cloud environment which control several clouds and avoids dependency on any one individual cloud. There are two layers in the Multi cloud environment: the bottom layer is the Inner- cloud, while the second layer is the Inter-cloud. In the Inter-Cloud, the Byzantine fault tolerance finds its place.

4.2 Introduction of Byzantine Protocols

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. 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.

BFT protocols are not suitable for single clouds. One of the 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.

4.3 DepSky System: Multi-Clouds Model

This will explain the recent work that has been done in the area of multi-clouds. Bessani et al 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.

4.3.1 DepSky Architecture

The DepSky architecture(figure2) 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.

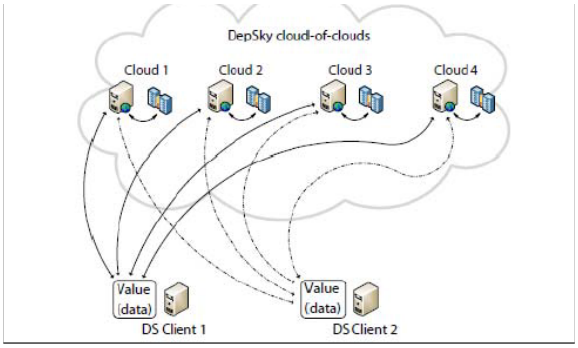

Figure 2.DepSky Architecture.

As the DepSky system deals with different cloud providers, the DepSky library deals with different cloud interface providers and consequently, the data format is accepted by each Cloud. The DepSky data model consists of three Abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation.

The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Bessani et al explain the difference between readers and writers for cloud storage. 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.

5. Proposed Work

We aim to provide a framework (figure 3) 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.

In relation to 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 the stored data in the cloud provider. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder.

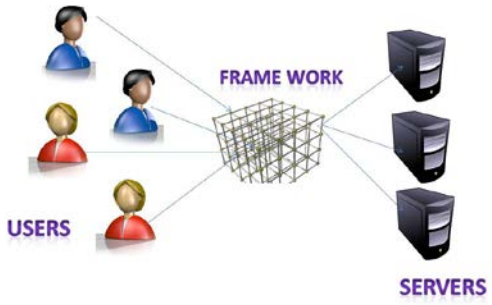

Figure 3.Multi-Cloud architecture

This depends on secret sharing algorithm with a polynomial function technique which claims that even with full knowledge of (k – 1) clouds, the service provider will not have any knowledge of secret value. 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. Therefore, if the attacker hacked one cloud provider's password or even two cloud provider's passwords, they still need to hack the third cloud provider (in the case where k = 3) to know the secret which is the worst case scenario. Hence, replicating data into multi-clouds by using a multi-share technique may reduce the risk of

data intrusion and increase data integrity. In other words, it will decrease the risk of the Hyper-Visor being hacked and Byzantine fault-tolerant data being stolen from the cloud provider. Regarding service availability risk or loss of data, if we replicate the data into different cloud providers, we could argue that the data loss risk will be reduced. If one cloud provider fails, we can still access our data live in other cloud providers.

6. Conclusion

It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently.

Furthermore, data intrusion leads Too many problems for the users of cloud computing. The purpose of this work is to address Multi-clouds to overcome the security risks and solutions. We support the migration to multi- clouds due to its ability to decrease security risks that affect the cloud computing user.

7. References

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

[2] 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.

[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] 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.

[5] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a- Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[6] Amazon, Amazon Web Services. Web services licensing agreement, October3,2006. [7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable datapossession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.

[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.

[9] K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80.

[10] 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.

[11] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.

[12] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp.81-86.

[13] C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed storage", DISC:Proc. 19thIntl.Conf. on Distributed Computing, 2005, pp. 497-498.

[14] M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998, pp. 173-186.

[15] G. Chockler, R. Guerraoui, I. Keidar and M. Vukolic, "Reliable distributed storage", Computer,

[16] A. Shamir, "How to share a secret", Communications of the ACM, 22(11), 1979, pp. 612-613.