International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 8, November 2014, PP 45-49
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Cloud Computing Security: A Shift from Cloud to Inter-Clouds

Shradha Modi, Bhuvnesh Nigam, Shivangi Mukhopadhyay, Prof. Anand Bone

Department of Computer Engineering
SKN Sinhgad Institute of Technology and Science, Lonavla

Abstract: *The usage of cloud computing has seen drastic growth in many organizations in the world. Cloud computing is use of computer resources that are delivered as a service over a network. Cloud computing provides many advantages such as sharing resources, low cost, improved accessibility. Ensuring the security in cloud computing environment is an issue of concern, because users mostly store sensitive information with the service providers. Dealing with single cloud involves the risk of accessibility failure and intervention of third party. Due to this a step towards inter-clouds or multi-clouds or clouds-of –clouds has born.*

General Term: *Security*

Keywords: *Cloud computing, Single computing, Inter-clouds, Depsky, Secret Sharing Algorithm*

1. INTRODUCTION

The usage of cloud computing has seen drastic growth in many organizations in the world. Subashini and Kavitha [1] discuss that small and medium companies focus on use of cloud computing services for many reasons as service provides low infra-structure cost and faster access to applications.

User data should not be affected by loss of availability, loss of corruption, loss of privacy or vendor lock-in problem. Dealing with single cloud involves the risk of accessibility failure and intervention of third party. In recent years a step towards inter-clouds or multi-clouds or cloud-of-clouds has born.

The paper mainly focuses on issues which are related to data security of cloud computing. Cloud users want to ignore an untrusted cloud provider protecting sensitive information from malicious insiders is a matter of high and urgent priority. Also the potential for shift from single to inter-cloud environment is examined are discussed along with security issue in single and inter-clouds in cloud computing environment.

1.1. Motivational Survey

Moving from single cloud to inter-clouds is reasonable and important for many reasons. Services of single clouds are still subject to interruption. The main purpose of moving to inter-clouds is to improve what was offered in single clouds by distributing reliability, trust and security among multi-cloud or inter-cloud providers. In addition, reliable distributed storage utilizes a subset of BFT techniques was suggested to be used in inter-clouds. A number of recent studies in this area have built protocols for inter-clouds or multi-clouds.

1.1.1. Existing System

The loss of availability of service is considered one of main limitations in cloud computing and it has been addressed by storing data on several clouds. Customers can use cryptographic methods to protect data in cloud. But if data is processed from many clients, data encryption cannot ensure privacy in cloud. As cloud can be attacked by third party. This system provides a secure storage cloud, but does not provide security of data in cloud model.

1.1.2. Proposed System

The work promotes user guarantee data confidentiality; it does not need code execution in their servers. User data does not get affected by loss of availability, loss of corruption of data, loss of privacy and vendor lock-in problem. User is able to access application environment which is located on server-side. Every user can access licensed version software for their work. This work aims to promote use of inter-cloud due to its ability to reduce security risks that affect the single cloud computing user.

2. BACKGROUND OF CLOUD COMPUTING

NIST [2] describes cloud computing as "a model for enabling convenient, on-demand network access to shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction".

2.1. Components of Cloud Computing

The cloud computing model consist of five characteristics, three delivery model, and four deployment models [2]. The five characteristics represents on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. The three delivery models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Deployment models are public, private, community and hybrid Cloud. The components are enlisted in Table 1.

Table1. *Cloud Computing Components*

Layer	Cloud computing components
Five Characteristics	On demand self-service Broad Network Access Resource pooling Rapid Elasticity Measured Services
Three Delivery Models	IaaS PaaS SaaS
Four Deployment Models	Public Private Community Hybrid

2.2. Features of Service Providers

Cloud service providers should be responsible for any security risks which affect customer's data and service infrastructure. A cloud service provider gives many services which can benefit its customer, it involves fast access to data from any location, scalability, pay-for-use, and data storage and data recovery, protection against hackers, on-demand security controls, and use of network and infrastructure facility [1]. Reliability and availability are additional benefits which are related to public cloud, in addition to low cost [3]. Data integrity and data confidentiality are most concerning issues when we talk about public clouds.

3. SECURITY RISKS IN SINGLE CLOUD

No doubt cloud service providers can offer many benefits to user, but security risks play a major role in cloud computing environment [4]. Online data sharing users are aware of potential of privacy loss [5]. Protecting private sensitive information like credit card details or different record from unwanted attackers and malicious insiders is of critical importance [6]. Shifting from database to large data centre comprise many challenges of data security, privacy and control issues concerned to data access from third party data theft, data loss, data integrity, confidentiality. Subashini and Kavitha [1] present some fundamental security challenges including data storage security, application security and other security issues related to third party.

The cloud services are provided by Internet. Any issue concerned to internet security will affect cloud services also. If cloud service provider looks after security in cloud infrastructure, issue of data transmission is yet not secured. Encryption techniques and different secure protocols are not at all enough to protect transmission of data in cloud. Intrusion of data in cloud over internet by cybercriminals and unwanted user needs to be addressed. The cloud computing environment needs to be secured for all clients [1].

3.1. Data Integrity

The most important issue concerned with cloud computing security is data integrity. The data which is stored inside cloud can suffer from damage during operations from one to other cloud storage providers. Cahinet al. [5] discusses that when multiple clients use cloud storage or when multiple devices are synchronized by same user, it is difficult to solve the data corruption issue. Cahinet al. [5]

proposed solution for it using Byzantine Fault Tolerant (BFT) replication protocol. Cahinet al. [6] claims that using BFT protocol in cloud is not suitable as servers belonging to cloud providers use same system installation and are located in same location. So, using BFT protocols across inter-clouds from different providers is beneficial.

3.2. Data Intrusion

This is another security risk which can occur with cloud provider. If someone again access to the account then data can be modified and services will be disabled. There is also a possibility of information stole.

3.3. Service Availability

This is also an issue of concern. Amazon [7] also mentions in its agreement that there is a possibility that service may not be available from time to time. Due to such term and condition only the customer will face the loss. The company won't be responsible for it in any way. Data authentication is extremely important as it ensures that returned data will be same as stored data.

4. INTER-CLOUDS COMPUTING SECURITY

4.1. Inter-clouds

Recent research surveys the inter-cloud environment. The bottom layer is inner-cloud, while second layer is inter-cloud. BFT comes into picture in inter-cloud [8]. This offers hardware, software and infrastructure redundancy which is necessary to optimize fault tolerance. Along with the benefits of steer traffic from different customer through parts of network.

4.2. Byzantine Protocol

Any fault related to intrusion tolerance along with faults in software or hardware or system crash is known as Byzantine Fault. The relation between Byzantine Fault Tolerant and cloud is considered one of major roles of distributed system. But again it is not suitable for single cloud.

4.3. Depsky Architecture

This architecture [9] gives the solution for availability and confidential data by the combination of inter-clouds, Byzantine qurum system and cryptographic secret sharing algorithm. The secret sharing algorithm provides security and Byzantine addresses fault tolerance. The Depsky architecture consist of four clouds where each cloud uses its own interface. The algorithm exists in client's machine as software library which communicates with each cloud [9].The figure 1 shows the architecture of Depsky.

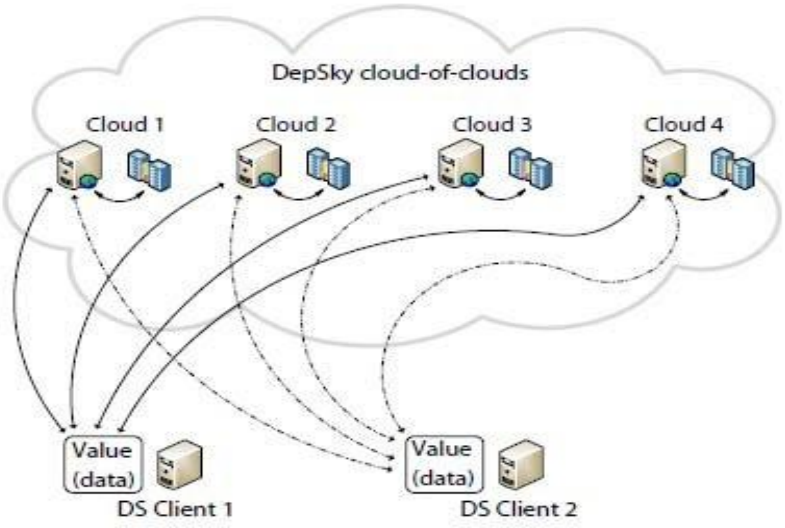

Figure1. *Depsky architecture*

The clouds are only for storage it has no code execution. Write and read operation in cloud are within Depsky library. The Depsky Data model has three levels of abstraction namely the conceptual data unit, generic data unit and data unit implementation. The Depsky system model comprises of three parts namely reader, writer and four cloud providers are task at client side.

4.3.1. Cloud Storage Providers in Depsky System Model

The Byzantine protocol has set of storage clouds (n). Here n=3f+1, where f is maximum clouds that can be fault. And Byzantine quorum protocols is created by subset of (n – f).

4.4. Secret Sharing Algorithm

In cryptography, secret sharing defines a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret [10]. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own [10].

Secret sharing algorithm gives tight control and removes single point vulnerability[10].The secret can only be reconstructed when the shares are combined together so individual key share holder cannot change/access the data[10].

Algorithm:

Goal is to divide some data D (e.g., the safe combination) into n pieces D_1, D_2 . . . D_n in such a way that:

Knowledge of any k or more D pieces makes D easily computable.

Knowledge of any k -1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called (k, n) threshold scheme.

If k=n then all participants are required together to reconstruct the secret.

4.5. Analysis of Inter-cloud

A shift from single to inter-cloud is important for many reasons discussed earlier. RACS that is, Redundant Array of Cloud Storage has RAID-like structure. RACS is for multiple cloud storage. The replication in cloud minimizes cost of switching providers. Also provides better fault tolerance RACS results the spread of storage among providers. HAIL which stands for High Availability and Integrity Layer is a protocol which controls multiple clouds. It provides software layer which address availability and integrity of data stored in multi-cloud.

These HAIL and RACS both has limitations concerned with it. Due to which their rule of not desirable. These limitations are not found in Depsky. So, it is appropriate to say that Depsky presents an experimental evaluation with many clouds, which is different from previous work on cloud.

5. ADVANTAGES AND LIMITATIONS

5.1. Advantages

Cloud computing is mostly economic. The sharing of resource decreases both the hardware and software cost. Besides it, it also provides more flexibility. And the service is available anytime and anywhere. It is beneficial in many ways as discussed earlier in the paper.

5.2. Limitations

Spreading resources across multiple data centers from same cloud provider addresses technical risk. Using public cloud has both technical and business risk, and both should factor in a multi-vendor strategy.

6. FUTURE ENHANCEMENT

Our target is to develop a framework which can supply secured cloud database which guarantees to prevent security risk. Depsky protocol enhances application sharing for all the critical data and sensitive information to avail good security in cloud we need to reduce the risk by secret sharing algorithm.

7. CONCLUSION

As the use of cloud computing is increasing day by day, the issue of security is becoming the matter of concern. The user wants the data to be secured in all possible ways. The work deals with research on single cloud and inter-clouds to look after security risk and solutions. If we compare single and

inter-clouds in terms of security inter-clouds is less popular. So, it has possibility of growth. We support the shift towards inter-clouds as it provides enhanced security.

REFERENCES

[1] 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.

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

[3] S. Kamara and K.Lauter, "Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptograpy and data security,2010, pp. 136-149.

[4] J. Viega, "Cloud computing and the common man", Computer, 42, 2009, pp. 106-108.

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

[6] H.Mei, J.Dawei, L.Guoliang and Z.Yuan, "Supporting Database Applications as a Service", ICDE'09:Proc. 25thIntl.Conf. on Data Engineering,2009, pp. 832-843.

[7] Amazon, Amazon Web Services.Web services licensing agreement, October3, 2006.

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

[9] 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.

[10] http://en.wikipedia.org/wiki/Shamir's_Secret_Sharing/.

AUTHORS' BIOGRAPHY

Shradha Modi is pursuing Bachelors of Engineering Degree from SKN Sinhgad Institute of Technology and Science, Lonavala. She is responsible for design analysis of system**.**

Bhuvnesh Nigam is pursuing Bachelors of Engineering Degree from SKN Sinhgad Institute of Technology and Science, Lonavala. He is responsible for giving module idea.

Shivangi Mukhopadhyay is pursuing Bachelors of Engineering Degree from SKN Sinhgad Institute of Technology and Science, Lonavala. She is responsible for overall idea of system**.**