International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
International Conference and Workshop on Communication, Computing and Virtualization (ICWCCV 2015) – www.ijais.org

Data Security in Multi-Cloud Environment – A Survey

Vaishali Tupe
M.E. Student, Dept. of Computer Engg,
Shah And Anchor Kutchhi Engg. College
Mumbai-400088, India

Vidyullata Devmane
Assistant Professor, Dept . of Computer Engg,
Shah And Anchor Kutchhi Engg. College,
Chembur,
Chembur, Mumbai-400088, India

,

ABSTRACT
Cloud computing is a powerful platform; it delivers IT (Information Technology) resources as a services over the Internet. It uses their own infrastructure to maintain customer's application and data. The cloud service provider offers platform, software and infrastructure as a service to the customer on pay per use basis. It may be either single cloud or multi cloud environment. Single cloud service provider is not reliable due to data security risk. In this survey paper various security issues in single cloud environment and requirement of switching from single cloud environment to multi cloud environment are discussed. Multi cloud environment has ability to reduce security risk of single cloud.

General Terms
Cloud computing, single cloud, multi cloud

Keywords
Data integrity, data intrusion, data availability

1. INTRODUCTION
cloud computing is "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" [11].

- Cloud computing used by many organization in order to avoid spending huge amount of capital on purchase and install there IT infrastructure or applications.
- Reducing burden on IT staff for providing better technical support.
- Can prevent obtaining excessive man power and training cost
- An immediate response of emergency situation, the cloud provider can offer 24/7 customer support

Cloud computing provide several benefits. Security is one the major issue in cloud computing environment. 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" [10].

This paper is focusing on the multi cloud environment to deal with the security issues raised while using the single cloud. The reminder of the paper is organized as follows. Section 2 describes related technologies used in cloud computing environment. Section 3 presents cloud components and examples of cloud providers. Section 4 describes various security issues in cloud computing environment. Section 5 discusses single cloud environment and its limitations. Section 6 describes analyses the new generation of cloud computing, that is, multi-clouds and recent solutions to address the security in cloud computing. Section 7 will gives the conclusions based on theoretical reading or survey.

2. RELATED TECHNOLOGIES
The several computing paradigms are peer to peer computing, cluster computing and greed computing. All this computing such as cluster computing, grid computing contributed in the development of cloud computing.

Grid computing is the segregation of resources from

Multiple sites so as to solve a problem that can't be solved by using the processing of a single computer [6].

Resources in grid geographically distributed across multiple administrative domain using own management and policies.

A cluster is a type of parallel and distributed system, which consists of a collection of inter-connected stand-alone computers working together as a single integrated computing resource [4].

Resources in cluster located in single administrative domain and managed by single entity.

A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers [4].

Cloud computing uses characteristics of both cluster and grid computing with its own special attributes which provide pool of dynamical scalable and virtual resources, storage services, and software on demand.

Characteristics of cloud computing are on demand self service, broad network access, resource pooling, rapid elasticity and measured service.

3. CLOUD ARCHITECTURE

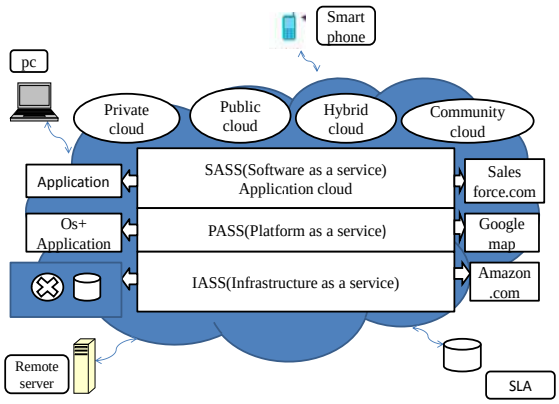

Figure 1: Cloud architecture

Figure1 presents cloud architecture. This model describes how cloud services made available to the customers. The three service delivery models are Infra structure as a service (Iass), Platform as a service (Pass) and Software as a service (Sass).

Iass provide infrastructure such as a processing memory, network bandwidth and storage on demand to the customer. Amazon web service is one of the most popular Iaas.

Saas provide ready software solution on which application hosted by cloud provider and made available to the customer over internet. An example of Saas is the Salesforce.com customer relationship management application.

Paas provide platform for building customer application. It provide software and development tool which are hosted by cloud service provider on their servers. Example is Google app engine.

Cloud deployment models are private cloud, public cloud, hybrid cloud and community cloud.

Private cloud is own and managed by special organization. Software such as VMware, Eucalyptus, and Open stack provides cloud functionality. Private cloud is safe and secure because data in private cloud handled by trusted user.

In the Public cloud the infrastructure is made available to the general public or a large group and is owned by an organization selling cloud services.

Hybrid cloud is combination of computing resources used by two or more public, private or community cloud

Community cloud shared across several organizations. It allows systems and services to accessible by group of organization or third party may exist on premises or off premises.

3.1 Cloud Service Providers

Cloud services are made available to customers with the help of cloud service providers. For example Amazon Elastic Compute Cloud (EC2) [1] provides a virtual computing environment that enables a user to run Linux-based applications. The user can either create a new Amazon Machine Image (AMI) containing the applications, libraries, data and associated configuration settings, or select from a library of globally available AMIs. The user then needs to upload the created or selected AMIs to Amazon Simple Storage Service (S3), before he can start, stop, and monitor instances of the uploaded AMIs.

- Payment for EC2 users are charged till the instances is alive.
- Payment for S3 users are charges for any data transfer (both download and upload) [2].

Google App Engine [7] allows a user to run web applications written using the Python programming language. Google App Engine also supports Application Programming Interfaces (APIs) for the data store, Google Accounts, URL fetch, image manipulation, and email services. Google App Engine also provides a web-based Administration Console for the user to easily manage his running web applications. Currently, Google App Engine is free to use with up to 500MB of storage and about 5 million page views per month.

Microsoft Azure [9] aims to provide an integrated development, hosting, and control Cloud computing environment so that software developers can easily create, host, manage, and scale both Web and non-web applications through Microsoft data centers. To achieve this aim, Microsoft Azure supports a comprehensive collection of proprietary development tools and protocols which consists of Live Services, Microsoft .NET Services, Microsoft SQL Services, Microsoft SharePoint Services, and Microsoft Dynamics CRM Services.

4. SECURITY ISSUES IN SINGLE CLOUD COMPUTING

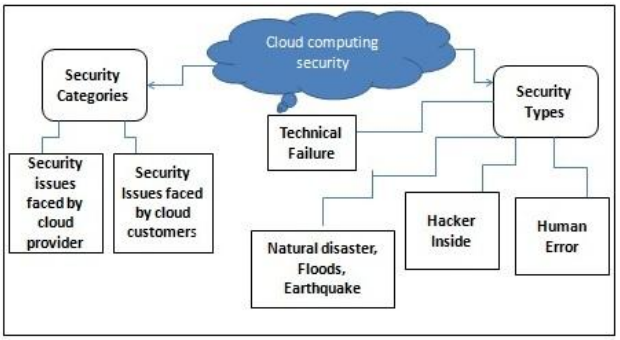

Figure 2: Security risk in single cloud environment

Various security are issued faced by cloud providers and users because moving data to data centers involves many security challenges such as confidentiality, integrity, availability data loss, and data theft. Security risk arises when a threat (an attacker) seeks to access data by exploiting an existing vulnerability. The cloud service provider can install countermeasures to reduce the impact of an attack.

- **Confidentiality**

Confidentiality refers to protect the data from unauthorized users. Cloud computing system offer (data and infrastructure) via public network. Therefore keeping all confidential data of user's secret in the cloud is fundamental requirement which will attract even more users consequently.

Data confidentiality can be achieved by using encryption method. Data can be encrypted before placing in cloud provider's server; only authorized user can access data using decryption method.

- **Integrity**

Data integrity refer to data cannot be altered by unauthorized person while transferring from or to cloud service provider.

Some of the elements used to ensure data integrity such as firewall, communication security management, intrusion detection service, and hash based method.

- **Availability**

Availability refer to data must be accessible to the authorized user in specified time. The concept of availability guarantee of service, performance and up time.
Some of the elements that are used to ensured availability are fault tolerance for data availability such as backup and redundant disk system, reliable and interoperable security process and network security mechanism [13].

4.1 Attacks on Data

- SQL injection attack

In this attack malicious code inserted by attacker in SQL statement and gives them access to steal data from organization. It can be avoid by sanitizing the user input.

- Service hijacking

Service hijacking is nothing but gaining unauthorized services. It includes various techniques like fraud, phishing and software exploitation.

- Social networking attacks

With the increased popularity of business and personal social networking sites the risk of advanced social engineering attacks are increased. Cloud computing systems are targeted due to their large customer data stores. Attackers can setup identities to gain trust, and use online information to determine relationships and roles of staff to prepare their attacks. A combination of technical attacks and social engineering attacks can be deployed against a target user by taking advantage of the people they know and the online social network they use [8].

For ensuring security in cloud environment two type of cloud architecture are used such as single cloud architecture and multi cloud architecture.

5. SINGLE CLOUD

Figure 3: Single cloud architecture

In single cloud architecture there is one main cloud server which accepts request from various users, if number of users are more and request services from such server then the performance of it will slow down, it may get hang sometimes. In this case there are huge overheads of managing large amount of data and for storing large amount of data high computing power server is required, so cost factor also matters.

In this environment availability of the data is not sure all the time. Due to any technical reason if server goes down then no will access data and customers will face the problems of data unavailability for that period. For example Amazon [3] mentions in its licensing agreement that it is possible the service might be unavailable from time to time. The user web service may terminate for any reason at any time if any user's file breaks the cloud storage policy. Both Google mail and Hotmail experienced service downtime recently [5].

For security purpose third party authentication is used in single cloud in which information stored on a cloud server is in encrypted form and using decryption techniques users' access this information. But this is a failure method because the hackers can easily steal the information by decrypting the text

5.1 Limitation of Single Cloud

- Data availability
- Needs high cost to maintain large amount of data
- Can fail to ensure the complete security from possible threats.

6. MULTI CLOUD

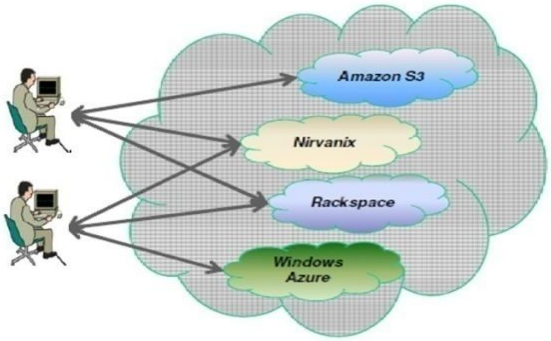

Figure 4: Multi cloud environment

To reduce all this security threats we are switching from single cloud to multi cloud. In multi cloud multiple cloud computing resources and services are used by customer in single heterogeneous architecture.

Multi cloud strategy is the simultaneous use of two or more cloud services to minimize the risk of widespread data loss or downtime due to a localized component failure in a cloud computing environment

6.1 Data Availability

In multi cloud environment there are multiple service providers where the customers store their data on multiple service provider servers so if any service provider's server will get down then data will be available from the other cloud.

6.2 Data Integrity

One of the most important issues related to cloud security risk is data integrity. The data store on cloud may suffer from data modification or data loss in transit or rest. To provide effective solution for data integrity for client's data in multi cloud environment is hash based approach (traditional method). In this method user's file are divided into numerous blocks. At any instant of the time files stored on two distinct clouds. For each cloud hash is calculated and the hash is furthermore maintained in the cloud. When any client request

for the cloud the file blocks retrieved from two cloud position by calculating hash function and matching with retained hash worth the integrity is verified.

6.3 Data Intrusion

Another issue related to cloud security risk is data intrusion. If anyone gains access to account password then they will access all account instances and resources, which allow to the hackers to modify or destroy the information inside the instance for stolen user account or hacker can also disable account instances. The data intrusion can be avoided by multigrade security level. The default security level is user name and password but this is not secured method because password can be easily hacked by hacker. So that second security level can be used. Here client has to login with his id and get password from server to get access to log on his listed mobile number and he has to login using that password. Another security level is biometric authentication which is more protected than above method.

6.4 Multi Cloud Benefits

- Data availability and scalability
- Hybridity – You can keep some applications on-premises and others on one or more public clouds, based on a variety of considerations, such as security, performance or cost optimization. For example, a hybrid cloud solution can also be used to provide faster service, particularly if your customers are located in different countries. Deploying your applications on a cloud that is closer to your customer's geographical location can result in better response time and performance.
- Autonomy – The ability to deploy applications on different cloud providers are the clear advantage of reducing dependency on a single vendor
- Meet different compliance and geographical needs – one want to be able to pick and choose where we want to deploy our applications based on compliance requirements, data protection laws, latency constraints and more.
- Extended capabilities – Different cloud providers support different platforms and offer constantly changing packages of capabilities. Features like Database as a Service, might not be supported by all cloud providers. It might be a good idea to shop around, comparing the various cloud offerings to identify which providers offer the best fit for user

7. CONCLUSIONS

In this paper various securities related to cloud computing environment are discussed. Data security is most important because most of the organization start using cloud computing services and store their valuable data on a cloud server. Customer does not want to lose their data as a result of security threat in cloud environment. The main reason of moving towards multi cloud is data availability. In single cloud environment data availability and security are not reliable. Multi cloud tries to decrease security risk using security methods such as hashing method, biometrics techniques, privacy preserving of data methods.

8. REFERENCES

[1] Amazon elastic compute cloud (EC2). http://www.amazon.com/ec2/ (18.07.08).

[2] Amazon simple storage service (S3). http://www.amazon.com/s3/ (18.07.08

[3] Amazon, Amazon Web Services. Web service licensing agreement, October3, 2006.

[4] Buyya Rajkumar, Yeo Chee Shin, Venugopal Srikumar, Broberg James and Brandic Ivona, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", Future Generation Computer Systems (2009), pp.599-616

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

[6] Gandotra Indu, Abrol Pawanesh, Gupta Pooja, Uppal Rohit and Singh Sandeep (2011), "Cloud Computing Over Cluster, Grid Computing: a Comparative Analysis", Journal of Grid and Distributed Computing, pp-01-04

[7] Google app engine. http://appengine.google.com (18.07.08).

[8] Jaydip Sen, "Security and Privacy Issues in Cloud Computing"; Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[9] Microsoft azure. http://www.microsoft.com/azure/ (30.10.08).

[10] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 2012, 45th Hawaii International Conference on System Sciences

[11] (National Institute Standard and Technology), http://www.nist.gov/itl/cloud/

[12] Sun network.com (Sun grid). http://www.network.com (18.07.08).

[13] Ronald L. Krutz Russell Dean Vine, "A Comprehensive Guide to Secure Cloud Computing".