International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue 3, June 2015
ISSN: 2395-3470
www.ijseas.com

An overview of cloud computing and security issues

S.Raghunath Reddy[1], Y.Rama Mohan[2], J.Swami Naik
G.PULLA REDDY ENGINEERING COLLEGE, KURNOOL

Abstract

Cloud computing is becoming an increasingly popular enterprise model because of its potential advantages where application services are provided through internet. It reduces the cost ownership, subscription based and pay-per-use services etc. computing offers Software as a service (SAAS, Platform as a service (PAAS), Infrastructure as a service (IAAS).This paper gives an overall survey on cloud computing, applications , security, computing resources over a network.

Keywords: cloud computing, security, risk, virtualization, attacks.

1. Introduction

The main intension of cloud computing is to provide services to the end users by storing, accessing of applications as well as data through a web rather than installing software in a computer in the office server. At the time of storing or accessing data we need high level security for the data. In this paper we have discussed some cloud attacks, cloud characteristics, cloud security, IT infrastructure as service and cloud applications. By providing applications programming interface (API) platforms hide the complexity and details of the infrastructure from users.

A. What is a cloud computing?

Basic definition of 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[1] .

B. Types of clouds

1. ***Private cloud***

A private cloud provides limited access to the single organization comprising multiple consumers or group. It is also called as Internal or corporate cloud.

2. ***Public cloud***

A public cloud can access to the cloud space with an internet connection and is open use by general public. It may be combination of owned, managed, business or government organization. It manages the resources like applications, storage available to the public in internet.

3. ***Community cloud***

A community cloud is shared among two or more organizations, a third party, or some combination of them that have similar cloud requirements.

4. ***Hybrid cloud***

A hybrid cloud is a combination of two or more cloud(public, private, community) and enables application portability which offers to move data and programs from one system to another.

International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue 3, May 2015
ISSN: 2395-3470
www.ijseas.com

PUBLIC vs. PRIVATE vs. HYBRID CLOUD STORAGE

Characteristic	Public cloud storage	Private cloud storage	Hybrid cloud storage
Scalability	Very high	Limited	Very high
Security	Good, but depends on the security measures of the service provider	Most secure, as all storage is on-premise	Very secure; integration options add an additional layer of security
Performance	Low to medium	Very good	Good, as active content is cached on-premise
Reliability	Medium; depends on Internet connectivity and service provider availability	High, as all equipment is on premise	Medium to high, as cached content is kept on-premise, but also depends on connectivity and service provider availability
Cost	Very good; pay-as-you-go model and no need for on-premise storage infrastructure	Good, but requires on-premise resources, such as data center space, electricity and cooling	Improved, since it allows moving some storage resources to a pay-as-you-go model

Private, public, hybrid cloud with characteristics

C.Cloud Favours or Service Models:

Space and resources will vary based on cloud provider and if we want to use the cloud for home and for business cloud type may vary. For business cloud provider will be charged pay as you used and also you can purchase more space in the cloud for business purpose. Mainly there are 3 types of services

1.**Software as a Service(SaaS)**

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[2] .various client devices can access applications through program interface and it is unnecessary to install software on devices.

Fig1. Examples of SaaS providers

2. **Platform as a Service(PaaS)**

The service provider gives access to the components that they require to develop and operate applications over the internet.

Fig2. Examples of PaaS providers

3. **Infrastructute as a Service(IaaS)**

The capability to provide storage, servers, networking etc(physical data center equipment)

Fig3. Examples of IaaS providers

D.Security Issues:

Suppose if we consider an organization they will use various models like public, private and hybrid clouds and services like infrastructure, platform and software as services. These models cause lot of security issues.

1.Multi-tenancy

Multi-tenancy provides sharing of resources, storage, memory etc for efficient utilization of resources with less cost. Sharing resources and applications with others either in physical or logical platform at cloud provider's space. It may be chance to loss the confidentiality and have a chance for possibility of attacks.

2.**Elasticity**

It enables users to use resources that are assigned previously to other tenant .It leads to confidentiality.

3.**Loss of control**

Location transparency enables organizations to unaware about the location of data and services from anywhere in the cloud. Organization have a chance to loss their data and not aware of security mechanism of provider.

4.**Data loss**

Multiple tenants uses the cloud, cloud does not provide data integrity and safety it results loss of data when updating and deletion of data without having backup.

E. Network security attacks

1. **Man in middle attack**

   It is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

2. **Distributed denial of service attacks**

   It is an attempt to make a machine or network resource unavailable to its intended users. A **DoS** attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

3. **Flooding attack problem**

   In cloud number of servers communicate with one another and transfers data , the requested job is authenticated and it requires lot of cpu utilization and is overloaded and it passed to another server, the usual process of system gets interrupted and system is flooded.

3. Techniques to secure data in cloud

1. Authentication and Identity
2. Data encryption
3 information integrity and privacy
4. Secure information management
5. Flooding attack solution

4. Conclusion

Cloud computing is the development trend of IT industry significantly by reducing the cost of present technologies. Both positive and negative are there in cloud computing .The cloud become a cost savings, productivity efficiency etc, but security is the major concern in the cloud .In this paper we have discussed lot of issues with cloud and specified some techniques to secure the data in the cloud. Some of the security issues will be solved by using these techniques.

REFERENCES

[1] NIST cloud definition, version 15 http://csrc.nist.gov/groups/SNS/cloudcomputing/

[2] Virtualization management tools (e.g from Citrix and VMware) are offering IaaS.

[3] Akhil Behl (2011), Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation).

[4] Akhil Behl & Kanika Behl (2012), An Analysis of Cloud Computing Security Issues.

[5] L. Ertaul, S. Singhal & G. Saldamli, Security Challenges In Cloud computing. [6] Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009,

[7] Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA(European Network and Information Security Agency), Crete, 2009.

[8] Cloud computing security forum http://cloudsecurity.org/ [7] Cloud Computing – A Practical Approach by Velte, Tata McGraw- Hill Edition (ISBN-13:978-0-07- 068351-8)

[9] Yashpalsinh jadeja & kirti modi cloud computing-concepts, architecture and challenges

[10] Satyendra singh rawat & Mr. Alpesh Soni ,A Survey of Various Techniques to Secure Cloud Storage

[11] R. Balasubramanian, Dr.M.Aramuthan Security Problems and Possible Security Approaches In Cloud Computing