ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Security Challenge in Cloud Computing

Ms Asiya Jaleel
M.Tech , Dept of CSE, Hyderabad, India
asiya.jaleel@gmail.com

Abstract

Cloud Computing is an internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customer on a pay –as—you-use basis. Users can access these services available on "Internet Cloud "without having any previous known how on managing the resources involved. But the major issue in the cloud computing is security. Several concerns which identify security requirements in cloud computing.

This paper brings out an introductory review on cloud computing ,various services and security challenges in cloud computing. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. This paper presents an elaborated study of IaaS components' security and determines vulnerabilities and countermeasures. Service Level Agreement should be considered very much importance.

Keywords: Cloud computing, SaaS,Paas, Iaas, Security Challenge.

Introduction

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. All the users or consumers need is to get the benefits of using the software or hardware of the computer like sending emails etc. Cloud computing is broken down into three segments: "application", "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses and individuals around the world. Cloud computing environments are likely to suffer from a number of known vulnerabilities, enabling attackers either to obtain computing services for free (attack against cloud providers), steal information from cloud users (attack against cloud customers data), or penetrate the infrastructure remaining in client premises through cloud connections (attack against cloud customer infrastructures). Typical examples of these attacks today are VoIP free calls, SQL injection, and drive by downloads.

Security Issues are of more concern to cloud service providers who are actually hosting the services.

Cloud Computing Architecture

Cloud computing means type of services provided to the customer .Services can be Data, security, Desktop, Software, platform, Infrastructure, IT, Testing, Hardware, Computing, Database, storage.

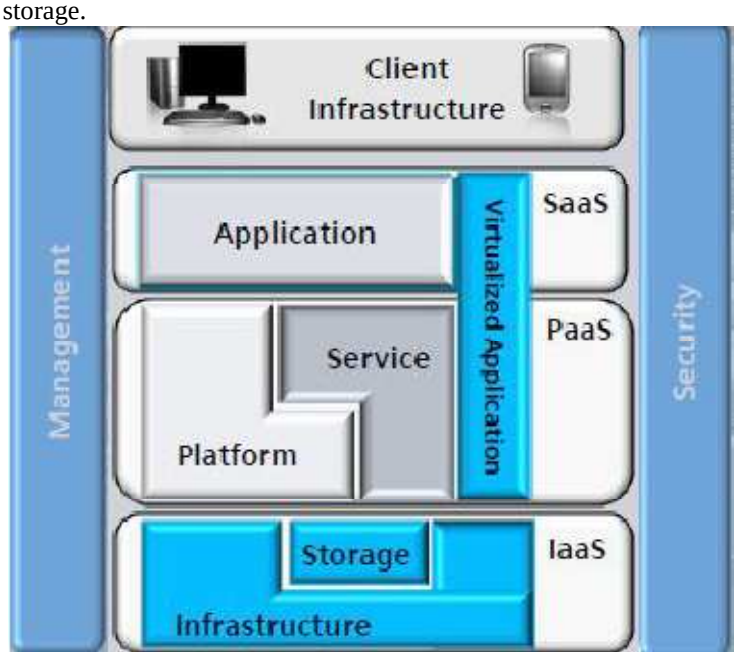

Fig 1: Cloud computing Architecture.

ISSN: 2277-9655
Impact Factor: 1.852

SAAS:

Saas is a software model provided by vendor through online service.

On the contrary, Centralization of data requires new/different security measures.

Examples of SaaS include Netflix, Intuit QuickBooks Online, Gmail, and Google

Docs. The four major advantages of Saas are:-

- Increased speed of deployment.
- Increased user adoption.
- Reduced support requirements.
- Lowered cost of implementation and upgrades.

PAAS:

PaaS enables companies to develop applications more quickly and efficiently in a cloud environment using programming languages and tools supported by the provider. The defining factor that makes PaaS unique is that it lets developers build and deploy web applications on a hosted infrastructure. It consumes cloud infrastructure. Every centralized system requires new/different security measures. Common examples of platforms include Windows™, Apple Mac OS X, and Linux for operating systems; Google Android, Windows Mobile, and Apple iOS for mobile computing; and Adobe AIR or the Microsoft .NET Framework for software frameworks.

IAAS:

This is the base layer of the cloud stack. It serves as a foundation for the other two layers, for their execution. The keyword behind this stack is Virtualization. Usually platform-independent; infrastructure costs are shared and thus reduced; service level agreements (SLAs); pay by usage; self-scaling. Avoid capital expenditure on hardware and human resources; reduced ROI risk; low barriers to entry; streamlined and automated scaling but disadvantages are Business efficiency and productivity largely depends on the vendor's capabilities; potentially greater long-term cost; centralization requires new/different security measures. With, a company can rent fundamental computing resources for deploying and running applications or storing data. IaaS enables fast deployment of applications, and improves the agility of IT services by instantly adding computing processing power and storage capacity when needed.

Cloud Computing Security Issues

In clouds rather than other issues security is the biggest issue. Due to this issue users are hesitating to use the clouds. According to a survey which is done in 2011 shows that 36% lack of cloud computing usage is due to security concerns. By Securing the Saas, PaaS and IaaS security issues indirectly we can secure the cloud system. Enough or adequate security can be achieved by solving these issues. Information security, Virtualized environment security issue and Communication security issues are some related issues. Information security is related to the important aspects of Availability, Confidentiality, and integrity.

Availability:

Availability means to ensure that users can use these services at any time at any place. It means availability of the infrastructure, software, or the data. All the Cloud computing systems like SaaS, PaaS, IaaS etc allows their users to access the cloud at anytime any place, to achieve this, cloud services should be available all the time.Virtual machines have capability to provide on demand services in terms of users. Most of the cloud computing systems provide cloud infrastructures and platforms based on virtual machines e.g. Amazon, S3, Xen so on. Amazon is using the virtual machines to rend resources (e.g. CPU cycles, storage capacity, memory etc.)Redundancy is another technique to provide the availability of the cloud. It means having multiple copies of the same data. Redundancy enhances the availability of the data or the system. Amazon and Google use this policy to provide availability

Confidentiality:

It means the data belongs to a particular user and it should not be revealed to any unauthorized party. It means only authorized parties or the systems can access to the data. One option for enhancing the confidentiality is encryption of the data. Encrypted data will be more secure rather than unencrypted. A Homomorphic cryptography (HC) can meet encryption challenge. A Homomorphic Cryptography ensures that operations performed on an encrypted text results in an encrypted version of the processed text. Encryption technique works while data is in transit mode, so the good solution of it is Tokenization. Tokenization means replacing sensitive data by dummy token. Translation of the token can be done at the client endpoint or at separate cloud provider.

Integrity:

Integrity means modification of data, referring of data, software and hardware. Integrity can be done only by authorized parties and in an authorized ways.

ISSN: 2277-9655
Impact Factor: 1.852

Integrity is a key aspect of security in cloud computing systems. It is also related to data loss and data stolen. As cloud systems are based on virtual machines, access points and number of entities increased and due to this integrity assurance and accuracy becomes crucial. One prominent solution is using of Zetta systems of storage which implements the Rain-6. Rain-6 is capable of recovering network failure, hard disk failure or corruption, power supply shortage etc it is able to tolerate three simultaneous failures (e.g. three disks failure or even a three entire nodes failure). Adding digital signature to the data enhances the data integrity (e.g. GFS (Google file system) and HDFS use this technique.

Conclusion

In this paper I have surveyed the major issues and challenges for cloud computing. I have classified the security challenges according to the three cloud service models: SaaS, PaaS, and IaaS. Furthermore, I analyzed existing solutions and provide some direction for how to handle the security threats. There are lots of issues related to security out of which we focused on information security, virtual machine security. By solving these issues cloud computing can get adequate security and user trust.

References

[1] http://cloudcom.org/
[2] http://ewh.ieee.org/ieee/ccem/
[3] http:// wikipedia.org/wiki/cloud computing
[4] http://www.vertical-cloud.com
[5] http://cloud computing.com
[6] http:// www.security challenges in cloud comptuing.com
[7] http://www. clean clouds.com.
[8] http://www.cloud.org.
[9] http:// www.cloudworld.com
[10]http:// www.security cloud.com