International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Issue 08, August 2015
www.ijates.com
ijates
ISSN 2348 - 7550

CLOUD COMPUTING: SECURITY THREATS AND MECHANISM

Vaishali Joshi[1], Lakshmi[2], Vivek Gupta[3]

[1,2,3]*Department of Computer Science Engineering, Acropolis Technical Campus, Indore*

ABSTRACT

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. Cloud computing is a significant advancement in the delivery of information technology and services. This paper explains the security threats and security mechanism in cloud computing, and outlines what are the major security concerns which are stopping the organization from moving completely to cloud.

Keywords: Cloud Computing, SaaS, PaaS, IaaS, Security, Threat, Mechanism

I. INTRODUCTION

Cloud computing is a significant advancement in the delivery of information technology and services. By providing on demand access to a shared pool of computing resources in a self-service, dynamically scaled and metered manner, cloud computing offers compelling advantages in speed, agility and efficiency. With Cloud Computing users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Five Essential Characteristics of cloud computing are:

- On-demand self service –Users are able to provision, monitor and manage computing resources as needed without the help of human administrators
- Broad network access – Computing services are delivered over standard networks and heterogeneous devices
- Rapid elasticity – IT resources are able to scale out and in quickly and on an as needed basis
- Resource pooling – IT resources are shared across multiple applications and tenants in a non-dedicated manner
- Measured service – IT resource utilization is tracked for each application and tenant, typically for public cloud billing or private cloud chargeback

1.1 Service model for Cloud Computing

- Infrastructure-as-a-Service (IaaS**)**

Infrastructure-as-a-Service is the first layer and foundation of cloud computing. Using this service model, you manage your applications, data, operating system, middleware and runtime. The service provider manages your virtualization, servers, networking and storage. This allows you to avoid expenditure on hardware and human capital; reduce your ROI risk; and streamline and automate scaling. An example of a typical need for this model

is someone who needs extra data space for processing power on occasion. Infrastructure-as-a-Service allows you to easily scale based on your needs and you only pay for the resources used..

- Platform-as-a-Service (PaaS)

This cloud service model could be considered the second layer. You manage your applications and data and the cloud vendor manages everything else. Benefits for using Platform-as-a-Service include streamlined version deployment and the ability to change or upgrade and minimize expenses. One popular Platform-as-a-Service is the Google app engine.A business with limited resources interested in app testing or development might find Platform-as-a-Service beneficial to eliminate costs of upkeep for hardware. In this model, your business benefits because it is not necessary to hire people to maintain these systems. A scalable processing center is available at your disposal to use as you need (again, you only pay for what you use).

- Software-as-a-Service (SaaS)

This is the final layer of the cloud services model. This allows your business to run programs in the cloud where all portions are managed by the cloud vendor. Your users will have assured compatibility and easier collaboration because all will be using the same software. Your company won't need to pay extra licensing fees and you can easily add new users. As consumers we interact with Software-as-a-Service based applications everyday without even realizing it. Examples of this are online banking and email such as Gmail and Hotmail.

Fig.1: Cloud Architecture

1.2 Cloud Structures

There are three primary deployment models for cloud services:

- Private clouds, whether operated and hosted by enterprise IT department or by an external provider, are for the exclusive use of the organization.
- Public clouds are open to any number of organizations and individual users on a shared basis. Using a public cloud minimizes initial capital investment and combines agility and efficiency with massive scalability.
- Hybrid clouds link private and public clouds, providing access to extra resources when the private cloud hits maximum utilization or, a hybrid cloud might split computing by tier between private and public clouds.

II. CLOUD COMPUTING SECURITY

There are major securities concerns which are stopping the organization from moving completely to cloud are:
Is my data secure on cloud?
Can other access my confidential data?
What if an attacker brings down my application which is hosted on cloud?

2.1 Key concept in information security is CIA (Confidentiality, Integrity, Availability) triad.

- Confidentiality: ensures that your data is confidential, unauthorized user can not access your data only authorized user can access the data.
- Integrity: ensures that your data remains as it is so no unauthorized user can change your data.
- Availability**:** ensures that your data, application & services are always available to authorized users.

2.1 Security Concerns in Cloud Computing

- Multitenancy: Single server host multiple VM

Same information is shared by different organization and VM might be collocated in a single server. When multiple organizations have various form of security policy how does cloud provider make sure that each company's security policy is fulfilled.

- Velocity of attack: Infrastructure is huge so the surface which is available for attack is huge that's why velocity of attack is also higher so because of this potential loss is also high, because if 1 VM is attack the entire infrastructure might get attack.
- Information assurance and data ownership**:** In case of cloud computing environment data and application are hosted by cloud service provider so the cloud service provider has access to data but the owner is not the CSP, the organization is owner so how to make sure that your data is accessed only by the authorized user and ensuring that the confidentiality is maintained.
- Data Privacy: To make sure that privacy of data is ensured in cloud environment because multiple enterprises and multiple users might be using the same infrastructure and might have access the data so it is important to make sure that privacy of data is maintained.

2.2 Cloud Security Threats

- VM theft: is vulnerability which enable attacker to copy a VM and use it for attacking the rest of infrastructure. VM is nothing but a file so VM is saved as a file in virtual environment so if a file doesn't have proper access privileges an authorized user can copy your VM file and use it for attacking. So hyper jacking enables attackers to install VM monitor that can take control of the underline server resources. Hyper wiser is a component that virtualized a server.
- Hyper jacking is an attack which takes control over the hyper wiser that creates the virtual environment within a VM host.
- Data Leakage: Confidential data stored on a third party cloud on is potentially vulnerable to unauthorized access or manipulation.
- Denial of service attack: It is an attempt to prevent legitimate users from accessing a resource or service.

III. CLOUD SECURITY MECHANISM

- Compute and network security
- Secure data at rest
- Identity and access management
- Risk analysis and compliance

3.1 Security at Compute Level

It includes

- Securing physical server
- Securing hypervisor
- Securing VMs
- VM isolation
- VM hardening
- Securing at guest OS level
- Guest OS hardening
- Securing at application level

  Application hardening

3.2 Securing Data-at-Rest

- Data-at- rest

  Data which is not being transferred over a network
- Encryption of Data-at-rest

  Provides confidentiality and integrity services

  Reduces legal liabilities of a CSP due to an unauthorized disclosure of data at its cloud.
- Full disk encryption is a key method to encrypt data at rest residing on a disk.

3.3 Identity and Access Management

- One time password

  Every new access requires new password

  A measure against password compromises.
- Federated identity management is provided as a service on cloud

  Enables organization to authenticate their users of cloud service using the chosen identity provider

  User identities across different organization can be managed together to enable collaboration on cloud.

3.4 Risk Assessment

- Aim to identify potential risks while operating on cloud environment

  Should be performed before moving to a cloud

  Used to determine the actual scope for cloud adoption
- Compliance

  Cloud adoption and operation for enterprise business need to abide by compliance policies

  Types of compliance
- Internal policy compliance

  Controls the nature of IT operations within organization

  Needs to maintain same compliance even when operating in cloud
- External Regulatory compliance

  Includes legal legislations and identity regulations

Controls the nature of IT operation related to flow of data out of an organization

May differs based on the type of information, business etc.

IV. CONCLUSION

Cloud computing represents an exciting opportunity to bring on-demand applications to customers in an environment of reduced risk and enhanced reliability. Cloud computing is particularly valuable to small and medium businesses, where effective and affordable IT tools are critical to helping them become more productive without spending lots of money on in-house resources and technical equipment. By adopting various mechanism of cloud computing security and take proper measure to avoid threats in cloud computing security, organization can easily adapt themselves in cloud environment.

REFERENCES

[1] Cloud Application Architectures: Building Application by George Reese.

[2] Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online by Michael Miller

[3] Grossman, R. L. The case of cloud computing, proc. of IEEE Educational Activities Department, Piscataway, NJ, USA vol. 11, Issue 2, pp. 23-37, March, 2009.

[4] M. D. Dikaiakos, D. Katsaros, G. Pallis, A. Vakali, P. Mehra: Guest Editors Introduction: "Cloud Computing, IEEE Internet Computing

[5] Luis M. Vaquero et al., A Break in the Clouds: Toward a Cloud Definition, ACM SIGCOMM Computer Communication Review, Volume 39, Issue 1 (January 2009)

[6] L. Kleinrock. A vision for the Internet. ST Journal of Research, 2(1):4-5, Nov. 2005.