Security Problems in Cloud Services

Aparajita&Diksha

Information Technology, Dronacharya College of Engg. Dronacharya College of Engg, Gurgaon, India

aparajitabd.508@gmail.com; dchoudhary1701@gmail.com

ABSTRACT-

Cloud computing is a set of IT services that are supplied to a customer over a network and with the ability to scale up or Finetune their service demands. Cloud computing services are rendered by a third party provider who has theinfrastructure. Its advantages include scalability, resilience, flexibility, efficiency and outsourcing noncore activities. Cloud computing offers a modern business model for governing bodies to take over IT services without upfront investment. Instate of the probable gains achieved from the cloud computing, due to security events and challenges associated with the organizations are slow in accepting it. Security is one of the major events which involve the maturation of cloud. The thought of handing important data to another company is challenging, hence that the consumers ask to interpret the hazards of data violation in this new environment.This paper includes an analysis of the security problems in cloud services, mainly focusing on the cloud computing service delivery model.

INTRODUCTION-

For years the Internet has been represented on network diagrams by a cloud symbol until 2008 when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud.

SECURITY ISSUES IN CLOUD COMPUTING

Cloud Deployments Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on thedemand . The Cloud Computing model has three main deployment models which are:

1. Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided
by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much
more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

2.Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via webapplications/web services, from an off-site third-party provider who shares resources and bills on
a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it
places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

3. Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure computing.

Security in the SPI model

The cloud model provides three types of services :

•Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

•Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.

•Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

With SaaS, the burden of security lies with the cloud provider. In part, this is because of the degree of abstraction, the SaaS model is based on a high degree of integrated functionality with minimal customer control or extensibility. By contrast, the PaaS model offers greater extensibility and greater customer control. Largely because of the relatively lower degree of abstraction, IaaS offers greater tenant or customer control over security than do PaaS or SaaS .

Before analyzing security challenges in Cloud Computing, we need to understand the relationships and dependencies between these cloud service models. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of these deep dependencies, any attack to any cloud service layer can compromise the upper layers. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. These relationships and dependencies between cloud models may also be a source of security risks. A SaaS provider may rent a development environment from a PaaS provider, which might also rent an infrastructure from an IaaS provider. Each provider is responsible for securing his own services, which may result in an inconsistent combination of security models. It also creates confusion over which service provider is responsible once an attack happens.

SUMMARY

While there are real benefits to using cloud computing, including some key security advantages, there are just as many if not more security challenges that prevent customers from committing to a cloud computing strategy. Ensuring that your data is securely protected both at rest and in transit, restricting and monitoring access to that data via user authentication and access logging, and adequately planning for the very real possibilities of compromised or inaccessible data due to data breaches or natural disasters are all key security challenges that a company must address when considering cloud computing providers.

References

[1] Subashini, 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): 1-11.

[2] Jensen, Meiko, et al. "On technical security issues in cloud computing." *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*. IEEE, 2009.

[3] Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and AtanuRakshit. "Cloud security issues." *Services Computing, 2009. SCC'09. IEEE International Conference on*. IEEE, 2009.

[4] Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and AtanuRakshit. "Cloud security issues." *Services Computing, 2009. SCC'09. IEEE International Conference on*. IEEE, 2009.

[5] Armbrust, Michael, et al. "A view of cloud computing." *Communications of the ACM* 53.4 (2010): 50-58.