FINAL REPORT AND PRESENTATION

Assessment item 4

MOHSIN ABDUL AZIZ
STUDENT ID: 11679894
Mohsinmazhar1996@gmail.com

Security Challenges in Service Model of Cloud Computing

NIST notes that cloud computing is defined as the model for providing its users with critical resources such as networks, servers, storage, and apps that can be supplied and released with the least management effort. Cloud computing provides five main features: rapid elasticity, self-service on demand, pooling of resources, wide network access, and measured services. It has three separate models of service delivery in which it offers the cloud users the application of the cloud provider to use (Hepsiba & Sathiaseelan, 2016).
Cloud computing provides business organizations with a "pay-as-you-go" model to deploy ready-to-use application services that save time, energy, and costs. Customers do not have to think about the underlying infrastructure architecture when using this model cloud, and are able to access the services at any time. In a cloud-computing model, data is allocated remotely on a separate shared computer instead of storing data across one physical machine, which can be easily accessed through a Web-based environment. It also offers the same infrastructure, including software and hardware services, to both its company and individual customers in this model.

Currently, cloud computing over the internet comprehensively encompasses all IT hosting business resources. These service models are divided into three distinct categories: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). Software-as-a-service (SaaS) allows cloud users to access cloud applications that are running, such as a web browser, on the cloud infrastructure. Consumers do not have to handle the underlying infrastructure architecture in the SaaS service model because all the latest hardware and software upgrades and installations are updated by the end of the application provider. For example, services such as Web applications provided by Google (Iqbal et al., 2016).

The Platform-as-a-Service (PaaS) model provides the platform for development in which cloud clients can build their own cloud-based application (Verma & Kaushal, 2011). PaaS helps its customers to develop, test and deploy IT services in the cloud world. This model allows businesses to rent virtual IT services and to test, create or even deploy a new application.

The infrastructure-as-a-service (IaaS) model provides on-demand, over the internet, fundamental computing, network, and storage services to its customers. IaaS allows end-users to scale up and scale down the assets as required. Compared to PaaS and SaaS, the lowest degree of resource management in the cloud is offered by IaaS (Knapp, 2020). Amazon S3, Ec2, and OpenNebula are examples, etc.
In a cloud computing paradigm, protection and privacy are considered a critical risk as more and more confidential cloud customer information is stored on the cloud. This paper provides a survey of the security issues that SaaS, PaaS, and IaaS cloud service models face.

Background

Cloud computing provides business organizations with a "pay-as-you-go" model to deploy ready-to-use application services that save time, energy, and costs. Consumers do not have to think about the underlying technology architecture when transferring their business data to the cloud, and are able to access services at any time. In a cloud-computing model, data is allocated remotely on a separate shared

computer instead of storing data across one physical machine, which can be easily accessed through a Web-based environment. It also offers the same infrastructure, including software and hardware services, to both its company and individual customers in this model.

CHALLENGES AND SECURITY ISSUES OF IAAS CLOUD MODEL:

IAAS cloud platform comes with many advantages, but also brings significant technological security and privacy considerations. In IAAS platform you rely on the vendor to provide you the functionality, which basically giving them your control. As soon as you give the control, you lose the access of the information.

A. Service Level Agreement (SLA)

Most of the resources on the cloud are not often fixed to any of the geo graphical location for instant specific data center. Using the SLA in the cloud provides the guarantee of acceptable quality of service level (QoS). SLA comprises of SLA monitoring, SLA negotiation, and SLA contract proposal. Contact and negotiation stage of SLA defines the roles and responsibility of each party i.e. consumer and the vendor. Any confusion and misunderstanding between the parties will lead to security of the system and make a room for the consumer exposure to vulnerabilities (Wesam-Dawoud et al., 2010).

B. Utility Computing

Utility computing plays an important role in the cloud computing deployment. It provides two essential benefits to the cloud consumer. Firstly, it reduces the overall cost instead of buying the whole resources, cloud consumer only needs to pay for the used resources which is referred as (pay-as-you-go). Secondly, it provides the consumer with the scalable system feature. The first most challenge of utility computing is in the complexity of cloud computing, for instant, Amazon needs to provides it services as metered services. These services are later used by the second level provider who also provides pay-as-you-go meter services (Wesam-Dawoud et al., 2010). This in result will turn out to be a multi-layer of utility which requires more management cost and efforts. Secondly, the system can be attacked by the attackers which are aiming to use the services without paying or they can further attack to drive the specific company bill to unmanageable level.

C. Cloud Software

There are many cloud software's available on the internet such as Nimbus and Eucalyptus etc. Cloud provider can't ensure the bugs and vulnerabilities in the available software. Cloud service provider use the API's such as SOAP, REST or XML etc. to perform the management task. A cloud consumer can use the Amazon EC2 toolkit to consume the cloud services. SOAP is considered as one of the most supported protocol for web services (Wesam-Dawoud et al., 2010). In SOAP, WS-Security serves as a standard extension for security. Well know attacks can be performed on the web services by using the XML signatures for the authentication or integrity protection which would affect the cloud services.

D. Insecure API's and Interfaces

Cloud consumer interact with the cloud services by using the interfaces which consists of API's. A set of different APIs can be exposed for instant monitoring and provisioning. Cloud services are mainly

dependent on the security of the basic API's. Any vulnerabilities in the APIs will lead the cloud services expose to liabilities (Vaquero et al., 2011).

E. Resource Sharing

In a cooperate environment resources are used by the single user. However, considering the cloud environment it is possible that the resource which is allocated to one corporation can be initiated on some physical infrastructure that can be allocated to the competitor corporation. For example, an instance of virtual machines is created and allocated to the corporation which is quite possible that some of the instances of the same virtual machine are also being used by the competitor organization. Which in result will lead to data leakage between the two corporations (Hay et al., 2011)

CHALLENGES AND SECURITY ISSUES OF SAAS CLOUD MODEL:

In this service model cloud consumers are totally dependent on the security provided by the service provider. Cloud provider need to make sure that multiple cloud consumers don't see each other data.

A. Privileged user access:

In this cloud model the cloud administrators can get as much information about the cloud consumer as much they want. Ask the cloud provider to provide only specific details on the venue of hiring and might oversight the privileged cloud administrator with their control over their access.

B. Data Segregation:

When you are moving your data to the cloud platform, you might don't know the exact location of your data storing hub. Probably, you don't even know the country where the data center is located. In this case ask the cloud provider for the commitment of storing and processing of your data in the specific jurisdictions, whether the cloud provider make the contractual commitment to follow the privacy on behalf of the cloud consumers.

C. Investigate Support:

In this platform the investigation of the illegal activities is nearly impossible, cloud services are difficult to investigate since data of multiple users might be co-located and this further be spread along with ever-changing set of data centers. (Popović & Hocenski, 2010)

D. Virtual Machine Security:

In the modern era of technology virtualized infrastructure are evolving rapidly. The virtual machines and the hypervisor used in the cloud platform can be exposed to vulnerabilities. These sorts of vulnerabilities are serious threat in multi-tenant platform where in case of failure of single virtual machine can exposed the data of all the cloud users on that physical server.

Virtualization is also one of the major parts of cloud, this main purpose is to make sure that different instances which are running on the same physical machine are isolated from each other but in today's world we can't see this sort of isolation completely. (Rashmi, et al., 2013).

CHALLENGES AND SECURITY ISSUES OF PAAS CLOUD MODEL:

Platform-as-a-service (PaaS) model provide the development environment in which the cloud customers can create their own application that will run on the cloud. PaaS enables its client to develop, test, and deploy IT services over the cloud environment. This model helps the business enterprises in renting out the virtual IT services as well as to test, develop, or even deploy a new application. As compare to SAAS and IAAS, PAAS cloud model provides more extensibility and greater cloud customers' control. There are still security threats to PAAS platform which are given below.

A. *Third-party relationships:*

PAAS platform not only support traditional programming language it also provides the consumers with third-party web services component for instant, Mashups. This component is the mixture of more than one source element which is merged into a single unit. Data and network security are one of the alarming security concerns in the mashups of PAAS delivery model. (Hashizume et al., 2013).

B. *Insecure Permission Threat:*

Insecure permission on the cloud platform is the major security threat to PAAS platform. The underlying permission on the user's data is not set appropriately due to which serious information leakage can happen. From the security point of view, it means that there are too much access of the data and not too little granted (Ramachandra et al., 2017).

C. *Underlying infrastructure security:*

In this platform most of the developers have not granted the access of the underlying layers. So, the cloud providers are the ones responsible for providing the security of the underlying infrastructure. Similarly, PaaS consumers is depending on the security of third-part service and web-hosted development tool (Hashizume et al., 2013).

Future Challenges

In conclusion, cloud computing has remained successful in attracting the customers, but there are still security and privacy threats which needs to be resolved in the future. Some of the future challenges of cloud computing includes account hijacking which is the cause of the weak password credentials. Another alarming threat is data scavenging, in this attack the attackers might be able to recover the lost data as the data remain on the device even after deleting it unless the device itself destroyed (Khan & Al-Yasiri, 2016). To counter this issue the vulnerabilities in the cloud needs to be resolved which cloud lead to serious threat in the future.

References:

Dawoud, W., Takouna, I., & Meinel, C. (2010, March). Infrastructure as a service security: Challenges and solutions. In 2010 the 7th International Conference on Informatics and Systems.

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing.

Hay, B., Nance, K., & Bishop, M. (2011, January). Storm clouds rising: security challenges for IaaS cloud computing.

Hepsiba, C. L., & Sathiaseelan, J. G. R. (2016). Security issues in service models of cloud computing.

Iqbal, S., Kiah, M. L. M., Anuar, N. B., Daghighi, B., Wahab, A. W. A., & Khan, S. (2016). Service delivery models of cloud computing: security issues and open challenges.

Khan, N., & Al-Yasiri, A. (2016). Identifying cloud security threats to strengthen cloud computing adoption framework.

Knapp, B. (2020). learn_iaas. Retrieved 1 October 2020, from https://www.ibm.com/cloud/learn/iaas.

Popović, K., & Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In The 33rd international convention mipro (pp. 344-349). IEEE.

Rai, R., Sahoo, G., & Mehfuz, S. (2013). Securing software as a service model of cloud computing: Issues and solutions.

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing.

Vaquero, L. M., Rodero-Merino, L., & Moráns, D. (2011). Locking the sky: a survey on IaaS cloud security.

Verma, A., & Kaushal, S. (2011, July). Cloud computing security issues and challenges: a survey. In International Conference on Advances in Computing and Communications (pp. 445-454).

Weekly Report Link:

https://thinkspace.csu.edu.au/11679894mohsinabdulaziz/