NAME - Piyush Agarwal
Enroll No. - 2017PUSBABCATOS248
Roll No - 2017BCTX1034
Subject - Cloud security

Batch - BCA(ITIMS&CT)
Section - B 2017-2020
SEM - VI
Faculty - Sandeep Kumar sharma

Q1 Explain the different cloud security Model in details.

As A cloud security delivery Models represent a specific resources offered by a cloud provider. Three common cloud computind delivery Model have become widly established a formalized.

① Software - as - a - service (SAAS)
② Platform - as - a - service (PAAS)
③ Infrastructure - as - a service (IAAS)

① SAAS => This Application are supplied by the ~~SS~~ CSP The Applications are Accessible from various client interface such As web browser the user does not manage or control the cloud infrastructure including servers. OS, storage or even individual Application capabilities with the possible exception of limited user-specific. Application configuration settings.

=> Rents the software on a subscription Basis.

=> Service include software hardware & support.

=> user Access the service through Authorized device

=> Suitable for a Company to Outsource hosting of. Apps.

② PAAS :- Paas user can deploy consumer created or acquired Applications using programming languages & tools supported by the CSP.

- under Affers the development environment to Application developer.
- provide, develops toolkits, building block, Payment hooks..

IAAS => Iaas offer the ability to provision processing Storage, Network other fundamental computing resources the consumer is able to deploy run arbitary Software which can include operating System & Application.

- Processing Power & Storage Service
- ~~typeer~~ hypervisior is at this level.

Q2 What are the host layer security issue in cloud Computing? Discuss any one issue in details.

Ans Two type of Security issue at the host level

(1) Attack1: Security concern with the hypervisor

(2) Attack 2: Securing virtual server.

Hypervisor is defined as controller called as virtual Machine manager [VMM] that allows multiple OS run on single Machine ~~at~~ a time if no. of OS running on hardware platform security issues get increased because single hardware unit is difficult to moniter Multiple operating system Et:.

Guest System tries to run Malicious code on the host system & get control of the system & Block other guest OS , even it can make change to Any guest OS Advance cloud protection system Can be development in order to monitor the guest VM And intern communication Among the various infrastructure components

Prevention Method

took Safe that Can provide generic Protection against Kernal mode Root kits.

Q3 What are the Application layer security issue in cloud computing ? Discuss Any one issue in detail ? .

Ans Six type of Security issue At Application level

① Attack 1 : Cookie poisioning
② Attack 2 : Backdoor & debug options
③ Attack 3 : Hidden field manipulation
④ Attack 4 : Google hacking
⑤ Attack 5 : SQL injection
⑥ Attack 6 : Cross site scripting Attack.

SQL Injection ⇒ Attackers inserted a malicious code into a standard SQL code And it Allow unauthorized person to download the entire database or intract it in other illicit ways The unauthorized user Can Access the sensitive data this will be avoided the usage of dynamically generated SQL in the code.

Prevention Method ⇒ Avoiding the ways of dynamicly generated sc the code.

Ques 4 Write a short note on ① Data ~~Availability~~ Integrity
② Data ~~privacy~~ Confidentially.

① Data ~~Availability~~ Integrity ⇒ Data integrity means protecting data from unauthorized deletion. modificiation or fabrication.

→ Data integrity ~~means~~ in the cloud system means Preseving the information integrity. The data should not lost or modified by unAuthorized uses.

→ Data integrity is the basis to provide cloud Computing service as Saas, Paas, IAas, Besides data storage of large-scaled data, cloud Computing environment ~~usa~~ usually Provides data Processing service.

② Data confidentiality :- Authenticiation & Access control issue in cloud computing ~~cloud~~ could be Addressed by increasing the cloud reliablity & trustworthiness

→ Data confidentiality is the important for user to store their private or confidential. data in the cloud Authencation & Access control strategies are used to ensure data confidentiality.

Ques 5 : Write the shot Note on ① Data Availability
② Data Privacy

① Data Availability => When Accidents Such as hard disk damage, IDC fire & network failure occur, the extent that user's data can be used or recovered And how the user verify their data by techniques rather that depending on the credit gurantee by the cloud service provider Alone.

② => This issue of storing data over the trans border services is a serious concern of clients because the cloud vendors are groverned by the local laws and therefore the cloud clients should be cognizant of those laws.

Data privacy => Privacy is the ability of an individual or group to seclude themselves or information about themseles & there by reveal them selectively.

Privacy has the following elements:-

① When :- A subject May be more Concerned About the current or Future information beign revaled the information From Past.

② How :- A user May be comfortable if his/her Friends can manully request his/her information but the user may not likely Alerts to be sent Automatically & preventely.

Extent => A user May rather have his/her information reported as an Ambigous region rather than Point.

Q-6 Explain term Cloud Security?

As cloud security are also known As cloud Computing security, consists of set of Policies, controls, procedures & technologies that work together to protect cloud-based System. data and infrastructure These security measured are configured to protect cloud data, support regulatory compliance And Protect customers privacy as well as setting Authentaction rules for individual users & devices.