**Chapter 13 – Cloud and IoT Security**

**TRUE/FALSE QUESTIONS:**

T F 1. Cloud computing gives you the ability to expand and reduce resources

according to your specific service requirement.

T F 2. IaaS provides service to customers in the form of software, specifically

application software, running on and accessible in the cloud.

T F 3. There is an increasingly prominent trend in many organizations to

move a substantial portion or even all IT operations to enterprise cloud computing.

T F 4. In a public cloud model the provider is responsible both for the cloud

infrastructure and for the control of data and operations within the

cloud.

T F 5. The major advantage of the public cloud is cost.

T F 6. A CSC can provide one or more of the cloud services to meet IT and

business requirements of a CSP.

T F 7. The three areas of support that a cloud broker can offer are service

intermediation, service aggregation and service arbitrage.

T F 8. NIST recommends selecting cloud providers that support strong

encryption, have appropriate redundancy mechanisms in place, employ authentication mechanisms, and offer subscribers sufficient visibility about mechanisms used to protect subscribers from other subscribers and the provider.

T F 9. Data must be secured while in transit, but not while in use or at rest.

T F 10. The term *platform as a service* has generally meant a package of

security services offered by a service provider that offloads much of

the security responsibility from an enterprise to the security service

provider.

T F 11. Security assessments are third-part audits of cloud services.

T F 12. An IPS is a set of automated tools designed to detect unauthorized

access to a host system.

T F 13. The security module for OpenStack is Keystone.

T F 14. The “smart” in a smart device is provided by a deeply embedded

actuator.

T F 15. A key element in providing security in an IoT deployment is the

gateway.

**MULTIPLE CHOICE QUESTIONS:**

1. Measured service and rapid elasticity are essential characteristics of \_\_\_\_\_\_\_\_\_.

A. resource pooling B. cloud computing

C. broad network access D. resource pooling

1. A \_\_\_\_\_\_\_\_\_\_ cloud provides service to customers in the form of a platform on which the customer’s applications can run.
2. broad network access B. infrastructure as a service
3. platform as a service D. resource pooling
4. The use of \_\_\_\_\_\_\_\_\_\_ avoids the complexity of software installation, maintenance, upgrades, and patches.
5. SaaS B. MaaS

C. PaaS D. IaaS

1. A \_\_\_\_\_\_\_\_\_\_ infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
2. community cloud B. private cloud

C. hybrid cloud D. public cloud

1. Examples of services delivered through the \_\_\_\_\_\_\_\_\_\_ include database on demand, e-mail on demand, and storage on demand.

1. hybrid cloud B. public cloud

C. private cloud D. community cloud

1. The \_\_\_\_\_\_\_\_\_ cloud deployment model is the most secure option.
2. public B. private

C. community D. hybrid

1. A \_\_\_\_\_\_\_\_\_\_ is an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between CSPs and cloud consumers.
2. cloud broker B. cloud carrier

C. cloud auditor D. cloud provider

1. A \_\_\_\_\_\_\_\_\_\_ is a person or organization that maintains a business relationship with, and uses service from, cloud providers.
2. loud auditor B. cloud service consumer

C. cloud broker D. cloud carrier

1. \_\_\_\_\_\_\_\_\_\_ is the monitoring, protecting, and verifying the security of data at rest, in motion, and in use.
2. Web security B. Security assessments

C. Intrusion management D. Data loss prevention

1. The core of \_\_\_\_\_\_\_\_\_\_\_ is the implementation of intrusion detection systems and intrusion prevention systems at entry points to the cloud and on servers in the cloud.
2. Intrusion management B. SIEM

C. security assessments D. web security

1. \_\_\_\_\_\_\_\_\_\_ comprise measures and mechanisms to ensure operational resiliency in the event of any service interruptions.
2. Data loss prevention
3. Security information and event management
4. Network security
5. Business continuity and disaster recovery
6. \_\_\_\_\_\_\_\_\_ is the management software module that controls VMs within the IaaS cloud computing platform.
7. Glance B. Nova

C. Swift D. Object

1. A \_\_\_\_\_\_\_\_\_\_ interconnects the IoT-enabled devices with the higher-level communication networks.
2. microcontroller B. gateway

C. carrier D. sensor

1. The most vulnerable part of an IoT is the \_\_\_\_\_\_\_\_\_\_ .
2. smart objects/embedded systems B. fog/edge network

C. core network D. data center/cloud

1. \_\_\_\_\_\_\_\_\_\_ has two operating modes, one tailored for single-source communication, and another tailored for multi-source broadcast communication.
2. Edge B. Keystone

C. OpenSource D. MiniSec

**SHORT ANSWER QUESTIONS:**

1. \_\_\_\_\_\_\_\_\_\_ is defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction”.
2. NIST SP 800-145 defines three service models: software as a service, platform as a service, and \_\_\_\_\_\_\_\_\_\_ as a service.
3. The four most prominent deployment models for cloud computing are public cloud, community cloud, hybrid cloud and \_\_\_\_\_\_\_\_\_ cloud.
4. The ­­­­­\_\_\_\_\_\_\_\_\_ cloud infrastructure is a composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.
5. A cloud \_\_\_\_\_\_\_\_\_\_ is a party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.
6. A cloud \_\_\_\_\_\_\_\_\_\_ is a networking facility that provides connectivity and transport of cloud services between cloud consumers and cloud service providers.
7. \_\_\_\_\_\_\_\_\_\_ includes people, processes and systems that are used to manage access to enterprise resources by assuring that the identity of an entity is verified, then granting the correct level of access based on this assured identity.
8. \_\_\_\_\_\_\_\_\_\_ aggregates log and event data from virtual and real networks, applications, and systems. This information is then correlated and analyzed to provide real-time reporting and alerting on information/events that may require intervention or other type of response.
9. \_\_\_\_\_\_\_\_\_\_\_ is an open-source software project of the OpenStack Foundation that aims to produce an open-source cloud operating system.
10. The \_\_\_\_\_\_\_\_\_\_ is a term that refers to the expanding interconnection of smart devices, ranging from appliances to tiny sensors.
11. With reference to the end systems supported, the Internet has gone through roughly four generations of deployment culminating in the IoT: information technology, operational technology, \_\_\_\_\_\_\_\_\_, and sensor/actuator technology.
12. The key components of an IoT-enabled device are: sensor, actuator, \_\_\_\_\_\_\_\_\_, transceiver and radio-frequency identification.
13. The core network, also referred to as a \_\_\_\_\_\_\_\_\_\_ network, connects geographically dispersed fog networks as well as provides access to other networks that are not part of the enterprise network.
14. MiniSec is an open-source security module that is part of the \_\_\_\_\_\_\_\_\_\_ operating system.
15. MiniSec is designed to meet the following requirements: data authentication, \_\_\_\_\_\_\_\_\_\_, replay protection, freshness, low energy overhead and resilient to lost messages.