

Name:

Enrolment No:



**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**End Semester Examination, May 2019**

**Course: Security in Cloud**

**Program: BTech – CSE (CCVT)**

**Course Code: CSIB 471**

**Semester: VIII**

**Time 03 hrs.**

**Max. Marks: 100**

**PART A (2\*30=60Marks)**

**1. Point out the correct statement.**

- a. Different types of cloud computing service models provide different levels of security services
- b. Adapting your on-premises systems to a cloud model requires that you determine what security mechanisms are required and mapping those to controls that exist in your chosen cloud service provider
- c. Data should be transferred and stored in an encrypted format for security purpose
- d. All of the mentioned

**2. Point out the wrong statement.**

- a. You can use proxy and brokerage services to separate clients from direct access to shared cloud storage
- b. Any distributed application has a much greater attack surface than an application that is closely held on a Local Area Network
- c. Cloud computing doesn't have vulnerabilities associated with Internet applications
- d. All of the mentioned

**3. Which of the following is not among the three important pillars of Security?**

- a. Authentication
- b. Confidentiality
- c. Availability
- d. Integrity

**4. What is the name of the organization helping to foster security standards for cloud computing?**

- a. Cloud Security Standards Working Group
- b. Cloud Security Alliance
- c. Cloud Security WatchDog
- d. Security in the Cloud Alliance

**5. Geographic distribution of data across a cloud provider's network is a problem for many enterprises because it:**

- a. Breaks compliance regulations
- b. Adds latency
- c. Raises security concerns
- d. Makes data recovery harder

- 6. What are some of the most common vulnerabilities that exist in a network or system?**
- Changing manufacturer, or recommended, settings of a newly installed application.
  - Additional unused features on commercial software packages.
  - Utilizing open source application code
  - Balancing security concerns with functionality and ease of use of a system.
- 7. What widely used service is built on cloud-computing technology?**
- Twitter
  - Skype
  - YouTube
  - All of the above
- 8. Which of these should a company consider before implementing cloud computing technology?**
- Employee satisfaction
  - Potential cost reduction
  - Information sensitivity
  - All of the above
- 9. Cloud computing embraces many concepts that were previously touted as the next big thing in information technology. Which of these is not an antecedent of the cloud?**
- Utility computing
  - Remote hosted services
  - Grid computing
  - Desktop computing
- 10. Which of these techniques is vital for creating cloud-computing data centers?**
- Virtualization
  - Transubstantiation
  - Cannibalization
  - Insubordination
- 11. An internal cloud is...**
- An overhanging threat
  - A career risk for a CIO
  - A cloud that sits behind a corporate firewall
  - The group of knowledge workers who use a social network for water-cooler gossip
- 12. What is Cloud Computing replacing?**
- Corporate data centers
  - Expensive personal computer hardware
  - Expensive software upgrades
  - All of the above
- 13. Which of the following is not a factor in securing the environment against an attack on security?**
- The system configuration
  - The network architecture
  - The business strategy of the company
  - The level of access provided to employees
- 14. Which of the following cloud concept is related to pooling and sharing of resources ?**
- Polymorphism
  - Virtualization

- c) Abstraction
  - d) Both a) and b)
15. Zomato formed a cloud for its all branches but due to its limited resources it obtained the services of AWS for extended provisioning and thus modified its cloud ; The cloud so formed is the example of \_\_\_\_\_
- a) Private cloud
  - b) Public cloud
  - c) Hybrid cloud
  - d) community cloud
16. Which of the following was one of the weaker aspects of early cloud computing service offerings?
- a) Logging
  - b) Integrity checking
  - c) Consistency checking
  - d) None of the mentioned
17. Which of the following are a common means for losing encrypted data?
- a) losing the keys
  - b) losing the encryption standard
  - c) losing the account
  - d) all of the mentioned
18. Which of the following is a key mechanism for protecting data?
- a) Access control
  - b) Auditing
  - c) Authentication
  - d) All of the mentioned
19. Point out the wrong statement.
- a) Securing data sent to, received from, and stored in the cloud is the single largest security concern
  - b) The problem with the data you store in the cloud is that it can be located anywhere in the cloud service provider's system
  - c) One and only approach to isolating storage in the cloud from direct client access is to create layered access to the data
  - d) All of the mentioned
20. Point out the correct statement.
- a) The cloud service model you choose does not determine the variety of security features, compliance auditing, and other requirements
  - b) To determine the particular security mechanisms you need, you must perform a mapping of the particular cloud service model to the particular application you are deploying
  - c) A security control model includes the security that you normally use for your applications only
  - d) All of the mentioned
21. What facet of cloud computing helps to guard against downtime and determines costs?
- A. Service-level agreements
  - B. Application programming interfaces
  - C. Virtual private networks
  - D. Bandwidth fees

22. Which of the following is used for Web performance management and load testing?
- a) VMware Hyperic
  - b) Webmetrics
  - c) Univa UD
  - d) Tapinsystems
23. Which of the following is considered an essential element in cloud computing by CSA?
- a) Multi-tenancy
  - b) Identity and access management
  - c) Virtualization
  - d) All of the mentioned
24. Which of the following services that need to be negotiated in Service Level Agreements?
- a) Logging
  - b) Auditing
  - c) Regulatory compliance
  - d) All of the mentioned
25. Which of the following service provider provides the least amount of built in security?
- a) SaaS
  - b) PaaS
  - c) IaaS
  - d) All of the mentioned
26. Which of the following is the operational domain of CSA?
- a) Scalability
  - b) Portability and interoperability
  - c) Flexibility
  - d) None of the mentioned
27. Cloud Services have a \_\_\_\_\_ relationship with their customers.
- A. Many-to-many
  - B. One-to-many
  - C. One-to-one
  - D. None of these
28. What's the most popular use case for public cloud computing today?
- A. Test and development
  - B. Website hosting
  - C. Disaster recovery
  - D. Business analytics
29. Virtual Machine Ware (VMware) is an example of
- A. Infrastructure Service
  - B. Platform Service
  - C. Software Service
  - D. None of these
30. Amazon Web Services is which type of cloud computing distribution model?
- A. Software as a Service (SAAS)
  - B. Platform as a Service (PAAS)
  - C. Infrastructure as a Service (IAAS)
  - D. None of these

**PART B (10\*4=40Marks)**

1. Discuss in detail the overview of Identity and Access management (IAM). [10marks]

2. Discuss the importance of data center security in cloud computing environment. Also discuss the physical and software security aspects in implementing data center security. **[10marks]**
  
3. Discuss the 'AAA' architecture with respect to Cloud Security along with its core components. **[10marks]**
  
4. Enlist and Explain the Four Protocol of SSL. **[10marks]**  
**OR**  
Differentiate between SSL and TLS security mechanisms.