MID-TERM EXAMINATION PAPER

FACULTY	:	**COMPUTER SCIENCE AND MULTIMEDIA**
COURSE	:	**BACHELOR OF INFORMATION TECHNOLOGY (BIT)**
YEAR/ SEMESTER	:	**THIRD YEAR / SIXTH SEMESTER**
MODULE TITLE	:	**CLOUD COMPUTING**
DATE	:	**4TH MARCH 2022**
TIME ALLOWED	:	**3 HOURS**
START	:	**6:30 AM – 9:30 AM**
SET	:	**A**

Instruction to candidates

1. This question paper has THREE (3) Section

2. Answer **ALL** questions in Section A, MCQ.

3. Answer **5** questions in Section B, MSAQ

4. Answer **2** questions in Section C, MEQ

5. No scripts or answer sheets are to be taken out of the Examination Hall.

6. For Section A, answer in the OMR form provided.

Do not open this question paper until instructed.

(Candidates are required to give their answers in their own words as far as practicable)

SECTION A

Multiple Choice Questions (30*1=30)

1. What type of computing technology refers to services and applications that typically run on a distributed network through virtualized resources?
    - a. Distributed Computing
    - b. Cloud Computing
    - c. Soft Computing
    - d. Parallel Computing

2. Which one of the following options can be considered as the Cloud?
    - a. Hadoop
    - b. Intranet
    - c. Web Applications
    - d. All of the mentioned

3. Cloud computing is a kind of abstraction which is based on the notion of combining physical resources and represents them as _____resources to users.
    - a. Real
    - b. Cloud
    - c. Virtual
    - d. None of the mentioned

4. Which of the following has many features of that is now known as cloud computing?
    - a. Web Service
    - b. Softwares
    - c. All of the mentioned
    - d. Internet

5. Which one of the following cloud concepts is related to sharing and pooling the resources?
    - a. Polymorphism
    - b. Virtualization
    - c. Abstraction
    - d. None of the mentioned

6. Which one of the following statements is not true?
    - a. The popularization of the Internet actually enabled most cloud computing systems.
    - b. Cloud computing makes the long-held dream of utility as a payment possible for you, with an infinitely scalable, universally available system, pay what you use.
    - c. Soft computing addresses a real paradigm in the way in which the system is deployed.
    - d. All of the mentioned

7. Which one of the following can be considered as a utility is a dream that dates from the beginning of the computing industry itself?
    - a. Computing
    - b. Model
    - c. Software
    - d. All of the mentioned

8. Which of the following is an essential concept related to Cloud?
    - a. Reliability
    - b. Abstraction
    - c. Productivity
    - d. All of the mentioned

9. Which one of the following is Cloud Platform by Amazon?
    - a. Azure
    - b. AWS

    c. Cloudera

    d. All of the mentioned

10. Which of the following statement is not true?

    a. Through cloud computing, one can begin with very small and become big in a rapid manner.

    b. All applications benefit from deployment in the Cloud.

    c. Cloud computing is revolutionary, even though the technology it is built on is evolutionary.

    d. None of the mentioned

11. In the Planning Phase, which of the following is the correct step for performing the analysis?

    a. Cloud Computing Value Proposition

    b. Cloud Computing Strategy Planning

    c. Business Architecture Development

    d. Both A and B

12. In which one of the following, a strategy record or Document is created respectively to the events, conditions a user may face while applying cloud computing mode.

    a. Cloud Computing Value Proposition

    b. Cloud Computing Strategy Planning

    c. Business Architecture Development

    d. Planning Phase

13. Which one of the following refers to the non-functional requirements like disaster recovery, security, reliability, etc.?

    a. Service Development   c. Plan Development

    b. Quality of service   d. Technical Service

14. Which one of the following is a phase of the Deployment process?

    a. Selecting Cloud Computing Provider

    b. IT Architecture Development

    c. Business Architecture Development

    d. Transformation Plan Development

15. This phase involves selecting a cloud provider based on the Service Level Agreement (SLA), which defines the level of service the provider receives.

    a. Maintenance and Technical Service

    b. Selecting Cloud Computing Provider

    c. Both A and B

    d. None of the above

16. Cloud computing architecture is a combination of?

a. service-oriented architecture and grid computing
b. Utility computing and event-driven architecture.
c. Service-oriented architecture and event-driven architecture.
d. Virtualization and event-driven architecture.

17. Which one of the following refers to the user's part of the Cloud Computing system?
    a. back End
    b. Management
    c. Infrastructure
    d. Front End

18. Which one of the following can be considered as the example of the Front-end?
    a. Web Browser
    b. Google Compute Engine
    c. Cisco Metapod
    d. Amazon Web Services

19. By whom is the backend commonly used?
    a. Client
    b. User
    c. Stockholders
    d. Service Provider

20. Through which, the backend and front-end are connected with each other?
    a. Browser
    b. Database
    c. Network
    d. Both A and B

21. Which of the following is one of the backend's built-in components of cloud computing?
    a. Security
    b. Application
    c. Storage
    d. Service

22. Which of the following provides the Graphic User Interface (GUI) for interaction with the cloud?
    a. Client
    b. Client Infrastructure
    c. Application
    d. Server

23. Which one of the following technology works behind the cloud computing platform?
    a. Virtualization
    b. SOA
    c. Grid Computing
    d. All of the above

24. Which one of the following is a kind of technique that allows sharing the single physical instance of an application or the resources among multiple organizations/customers?
    a. Virtualization
    b. Service-Oriented Architecture
    c. Grid Computing
    d. Utility Computing

25. Which one of the following statements is true about Virtualization?
    a. It provides a logical name for a physical resource, and on-demand provides an indicator of that physical resource.
    b. In Virtualization, we analyze the strategy related problems that customers may face.
    c. In Virtualization, it is necessary to compile the Multitenant properly.
    d. All of the above

26. In Virtualization, which architecture provides the virtual isolation between the several tenants?
    a. IT Architecture
    b. Multitenant
    c. Deployment
    d. Business Architecture
27. On which one of the following utility computing is based?
    a. Grid Computing Model
    b. SOA Model
    c. virtual isolation Model
    d. Pay-Per-Use Model

28. In Grid Computing, which types of computer resources are there?
    a. heterogeneous dispersed.
    b. geographically dispersed.
    c. Both A and B
    d. None of the above
29. Which one of the following given programs provides the isolation (abstraction) and partitioning?
    a. System hypervisor
    b. Software hypervisor
    c. Hardware hypervisor
    d. Virtualization hypervisor

30. Which one of the following runs on Xen Hypervisor?
    a. Azure
    b. AWS EC2
    c. C AWS EC3
    d. All of the above

SECTION B
Short Question Answer
Attempt any five (5) questions out of eight (8) questions   **(5*6=30)**

1. Describe cloud-based services. What are the challenges in cloud computing?

2. How grid computing differs from cloud computing? Justify what the elasticity and multitenancy properties of cloud computing mean?

3. What do you mean by virtualization? What is the role of virtualization in cloud computing?

4. What is the cloud security challenge? How risks can be handles in cloud computing?

5. Discuss about disasters in cloud. How intrusions are detected in cloud?

6. How can you design the security architecture in cloud? Explain.

7. Explain the different approaches for enforcing host security in a cloud environment.

8. Differentiate between each of the private, public and hybrid cloud models with suitable examples.

SECTION C
Long Question Answer
Attempt any two (2) questions out of three (3) questions   **(2*20=40)**

1. Discuss Jericho Cloud Cube Model. How do the Jericho Cloud Cube model dimensions like parameterized, de-parameterized, and proprietary, open differentiate the cloud formations from each other?

2. What do you mean by disaster recovery? How recovery point objective differs from recovery time objective?

3. **Case Study. (20)**

   Cloud computing is reshaping enterprise network architectures and infrastructures. It refers to applications delivered as services over the Internet as well as the hardware and systems software in data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS) which had its roots in software-oriented Architecture (SOA) concepts that began shaping enterprise network roadmaps in the early 2000s. IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) are other types of cloud computing services that are available to business customers.

Cloud computing fosters the notion of computing as a utility that can be consumed by businesses on demand in a manner that is similar to other services (e.g. electricity, municipal water) from traditional utilities. It has the potential to reshape much of the IT industry by giving businesses the option of running business software applications fully on-premises, fully in "the cloud" or some combination of these two extremes. These are choices that businesses have not had until recently and many companies are still coming to grips with this new computing landscape.

Security is important to any computing infrastructure. Companies go to great lengths to secure on-premises computing systems, so it is not surprising that security looms as a major consideration when augmenting or replacing on-premises systems with cloud services. Allaying security concerns is frequently a prerequisite for further discussions about migrating part or all of an organization's computing architecture to the cloud.

Availability is another major concern: "How will we operate if we can't access the Internet? What if our customers can't access the cloud to place orders?" are common questions. Generally speaking, such questions only arise when businesses contemplate moving core transaction processing, such as ERP systems, and other mission-critical applications to the cloud. Companies have traditionally demonstrated less concern about migrating high maintenance applications such as e-mail and payroll to cloud service providers even though such applications hold sensitive information.

Security Issues and Concerns Auditability is a concern for many organizations, especially those who must comply with Sarbanes-Oxley and/or Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) regulations. The suitability of their data must be ensured whether it is stored on-premises or moved to the cloud. Before moving critical infrastructure to the cloud, businesses should do diligence on security threats both from outside and inside the cloud. Many of the security issues associated with protecting clouds from outside threats are similar to those that have traditionally faced centralized data centers. In the cloud, however, responsibility for assuring adequate security is frequently shared among users, vendors, and any third-party firms that users rely on for security-sensitive software or configurations. Cloud users are responsible for application-level security.

Cloud vendors are responsible for physical security and some software security such as enforcing external firewall policies. Security for intermediate layers of the software stack is shared between users and vendors. A security risk that can be overlooked by companies considering a migration to the cloud is that posed by sharing vendor resources with other cloud users. Cloud providers must guard against theft or denial-of-service attacks by their users and users need to be protected from one another.

Virtualization can be a powerful mechanism for addressing these potential risks because it protects against most attempts by users to attack one another or the provider's infrastructure. However, not all resources are virtualized, and not all virtualization environments are bug-free. Incorrect virtualization may allow user code to access to sensitive portions of the provider's infrastructure or the resources of other users. Once again, these security issues are not unique to the cloud and are similar to those involved in managing non-cloud data centers, where different applications need to be protected from one another.

Another security concern that businesses should consider is the extent to which subscribers are protected against the provider, especially in the area of inadvertent data loss. For example, in the event of provider infrastructure improvements, what happens to hardware that is retired or replaced? It is easy to imagine a hard disk being disposed of without being properly wiped clean of subscriber data. It is also easy to imagine permissions bugs or errors that make subscriber data visible to unauthorized users. User-level encryption may be an important self-help mechanism for subscribers, but businesses should ensure that other protections are in place to avoid inadvertent data loss.

Addressing Cloud Computer Security Concerns Numerous documents have been developed to guide businesses thinking about the security issues associated with cloud computing. Even NIST has weighed in on these issues. NIST's recommendations systematically consider each of the major types of cloud services consumed by businesses including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). While security issues vary somewhat depending on the type of cloud service, there are multiple NIST recommendations that are independent of service type. Not surprisingly, 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.

As more businesses incorporate cloud services into their enterprise network infrastructures, cloud computing security will persist as an important issue. Examples of cloud computing security failures have to potential to have a chilling effect on business interest in cloud services and this is inspiring service providers to be serious about incorporating security mechanisms that will allay concerns of potential subscribers. Some service providers have moved their operations to Tier 4 data centers to address user concerns about availability and redundancy. Because so many businesses remain reluctant to embrace cloud computing in a big way, cloud service providers will have to continue to work hard to convince potential customers that computing support for core business processes and mission-critical applications can be moved safely and securely to the cloud.

Questions:

a. Do some research to identify businesses that have suffered because of cloud security weaknesses or failures. What can companies who are contemplating cloud computing services learn from the negative experiences of these businesses?
b. Do some Internet research on security mechanisms associated with virtualization. How can virtualization be used by cloud service providers to protect subscriber data?
c. Choose one of the following cloud services categories: SaaS, IaaS, PaaS. Do some Internet research that focuses the security issues associated with the selected cloud service category. Summarize the major security risks associated with the cloud service category and identify mechanisms that can be used to address these risks.

****BEST OF LUCK****