Name of the Subject: Technology Trends in IT

Course Code: 504 **Semester: I**

Unit-3: Cloud Computing (MCQ)

1. What is Cloud Computing?

A) A network of servers located in a single data center.

B) On-demand delivery of IT resources over the internet with pay-as-you-go pricing.

C) A method for physically storing data on local hard drives.

D) A process of upgrading hardware devices in an organization.

Answer: B) On-demand delivery of IT resources over the internet with pay-as-you-go pricing.

2. Why are cloud services popular among businesses and individuals?

A) They require high initial costs and long-term commitments.

B) They provide greater flexibility, scalability, and reduced costs.

C) They are only accessible within an organization's network.

D) They eliminate the need for an internet connection.

Answer: B) They provide greater flexibility, scalability, and reduced costs.

3. Which of the following is NOT an advantage of cloud computing?

A) Increased flexibility and scalability.

B) Data security risks.

C) Reduced IT infrastructure costs.

D) Accessibility from any internet-enabled device.

Answer: B) Data security risks.

4. What is a key characteristic of cloud computing that allows users to access resources as needed?

A) Resource pooling

B) Broad network access

C) On-demand self-service

D) Rapid elasticity

Answer: C) On-demand self-service

Name of the Subject: Technology Trends in IT

Course Code: 504 Semester: I

5. Which of the following is a common service model in cloud computing?

A) Hardware as a Service (HaaS)

B) Platform as a Service (PaaS)

C) Data as a Service (DaaS)

D) Device as a Service (DaaS)

Answer: B) Platform as a Service (PaaS)

6. What is the difference between Public Cloud and Private Cloud deployments?

A) Public clouds are only accessible by an organization's employees, while private clouds are accessible by anyone.

B) Public clouds are owned by third-party providers and available to the public, while private clouds are dedicated to one organization.

C) Private clouds offer better scalability than public clouds.

D) Public clouds are free, while private clouds have high costs.

Answer: B) Public clouds are owned by third-party providers and available to the public, while private clouds are dedicated to one organization.

7. What is a common privacy risk associated with cloud computing?

A) Lack of data redundancy

B) Limited data access

C) Potential for unauthorized access to sensitive information

D) Requirement for large physical storage

Answer: C) Potential for unauthorized access to sensitive information

Unit-4: Cyber Security (MCQ)

8. What is Cyber Security?

A) Protecting software from bugs and updates.

B) The practice of defending computers, servers, mobile devices, and networks from digital attacks.

C) Managing cloud computing costs effectively.

D) Installing antivirus software on all devices.

Answer: B) The practice of defending computers, servers, mobile devices, and networks from digital attacks.

9. Which of the following is considered a common risk in cyber security?

A) Fast internet speeds

B) Phishing and social engineering attacks

C) Increased processing power

D) Low battery life on devices

Answer: B) Phishing and social engineering attacks

10. What is malicious code?

A) Code written to improve network speed.

B) Any code designed to damage, disrupt, or gain unauthorized access to a computer system.

C) Code that enhances data encryption.

D) Software update files.

Answer: B) Any code designed to damage, disrupt, or gain unauthorized access to a computer system.

11. What is the primary goal of a hacker, attacker, or intruder in cyber security?

A) To develop new software tools.

B) To gain unauthorized access to information or disrupt operations.

C) To back up data securely.

D) To test network speeds.

Answer: B) To gain unauthorized access to information or disrupt operations.

12. Which of the following is a fundamental principle of cyber security?

A) Integrity, Availability, and Confidentiality

B) Accessibility, Speed, and Usability

C) Cost Reduction, Redundancy, and Accessibility

D) Confidentiality, Usability, and Upgradability

Answer: A) Integrity, Availability, and Confidentiality

13. In the context of Information Security (IS) within Lifecycle Management, which stage involves the regular monitoring of systems and networks?

A) Planning

B) Development

C) Maintenance and Operations

D) Decommissioning

Answer: C) Maintenance and Operations

14. What is the main goal of an incident response team in cyber security?

A) To increase the speed of data transfers

B) To mitigate the impact of a cyber incident and restore normal operations

C) To install new security hardware

D) To design a new system architecture

Answer: B) To mitigate the impact of a cyber incident and restore normal operations

15. Which of the following is a key area of focus for future cyber security implications and evolving technologies?

A) Development of low-cost hardware devices

B) Use of AI and machine learning to detect threats

C) Reducing screen sizes on mobile devices

D) Eliminating encryption algorithms

Answer: B) Use of AI and machine learning to detect threats

Unit-5: Wearable Technologies (MCQ)

16. What is Wearable Technology?

A) A type of technology that can be worn on the body and includes devices that connect to the internet or other devices.

B) Technology that only functions when connected to a desktop computer.

C) A form of artificial intelligence that creates wearable software.

D) A system designed exclusively for video streaming.

Answer: A) A type of technology that can be worn on the body and includes devices that connect to the internet or other devices.

17. Which of the following is a common application of wearable technology in healthcare?

A) Providing remote technical support for computer systems.

B) Tracking physical activity and monitoring vital signs.

C) Streaming online movies and games.

D) Developing mobile applications for social media.

Answer: B) Tracking physical activity and monitoring vital signs.

18. Which wearable device is primarily used to measure physical activity and health metrics?

A) Virtual Reality (VR) headset

B) Smartwatch

C) Wireless headphones

D) Tablet

Answer: B) Smartwatch

19. What is a significant challenge facing wearable technology?

A) High battery life and small device sizes

B) Data privacy and security concerns

C) Low production costs

D) No demand for wearable technology in healthcare

Answer: B) Data privacy and security concerns

20. Which of the following is NOT a common wearable device?

A) Fitness tracker

B) Smart glasses

C) Desktop computer

D) Smart ring

Answer: C) Desktop computer

21. In what field is wearable technology frequently applied to monitor employee safety and performance?

A) Hospitality industry

B) Manufacturing and industrial sectors

C) Fashion industry

D) Entertainment industry

Answer: B) Manufacturing and industrial sectors

22. How do wearable devices commonly connect to other devices or networks?

A) Through wired connections only

B) Using Bluetooth, Wi-Fi, or NFC

C) By satellite connections exclusively

D) Via USB cables

Answer: B) Using Bluetooth, Wi-Fi, or NFC

23. Which wearable device is designed to provide an immersive virtual experience and is popular in gaming?

A) Smartwatch

B) Virtual Reality (VR) headset

C) Fitness tracker

D) Smart ring

Answer: B) Virtual Reality (VR) headset

SHORT ANSWERS:

Unit-03: Cloud Computing for (Q.2)

1. What is cloud computing, and why is it significant?

Cloud computing is a technology that provides on-demand access to computing resources like storage, servers, and applications over the internet. It allows organizations to avoid heavy upfront infrastructure costs, relying instead on remote servers managed by cloud providers, which helps streamline operations and focus on core business needs.

2. Why have cloud services become popular in recent years?

Cloud services are popular due to their flexibility, cost savings, and scalability. By using cloud services, organizations can pay only for what they use, easily scale resources to match demand, and support remote access, which is crucial for distributed teams and remote work environments.

3. What are the main advantages of using cloud computing?

Key advantages of cloud computing include reduced IT costs, as it eliminates the need for physical infrastructure; enhanced collaboration through shared access to resources; and greater flexibility, enabling businesses to rapidly adjust to changing demands without large investments in hardware.

---

4. What are the primary cloud service models, and what does each offer?

The three main cloud service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides virtualized hardware resources like storage and networking, ideal for scalable infrastructure. PaaS offers a development environment, allowing developers to build and deploy applications without managing the underlying infrastructure. SaaS delivers software applications over the internet, enabling users to access tools like email and CRM platforms directly from their browsers without installation or maintenance requirements.

5. What privacy and security risks exist with cloud computing?

Cloud computing poses privacy risks due to shared environments, which can lead to unauthorized access to sensitive data and data breaches. Users must trust cloud providers to implement strong security measures since data is stored and managed off-site. Other risks include data loss, regulatory compliance issues, and potential access by third parties, which can compromise confidentiality. Therefore, evaluating the cloud provider's security policies and compliance standards is essential for protecting sensitive information.

Unit-04: Cyber Security for (Q.3)

1. What is cyber security, and why is it important?

Cyber security is the practice of protecting computer systems, networks, and data from unauthorized access, damage, or attacks. It is crucial because cyber threats are increasing in complexity, posing risks to individuals and organizations alike. Effective cyber security measures help protect sensitive data and ensure the integrity and availability of digital services.

2. What are common types of risks associated with cyber security?

Common cyber security risks include phishing attacks, malware infections, data breaches, and denial-of-service attacks. These threats can lead to data theft, system disruptions, and financial loss, making it essential for organizations to adopt preventive measures to safeguard their networks and data.

3. Who are hackers, attackers, and intruders in the context of cyber security?

Hackers, attackers, and intruders are individuals or groups that attempt to gain unauthorized access to systems or networks. While some hackers are ethical (white-hat hackers) who help improve security, others (black-hat hackers) exploit vulnerabilities for personal gain, often causing harm by stealing data, damaging systems, or launching cyber attacks.

---

4. What are the fundamental principles of cyber security, and how do they protect information?

The core principles of cyber security are confidentiality, integrity, and availability, often referred to as the CIA triad. Confidentiality ensures that sensitive information is accessible only to authorized users, integrity safeguards data from unauthorized changes, and availability ensures resources are accessible when needed. Together, these principles form a foundation for protecting information from unauthorized access and threats.

5. What role does incident response play in cyber security, and why is it critical?

Incident response involves identifying, managing, and resolving cyber security incidents to minimize damage and recover quickly. A well-planned incident response strategy enables organizations to detect threats early, mitigate their impact, and restore normal operations. It is crucial for limiting data loss, protecting sensitive information, and maintaining customer trust. Effective incident response also helps organizations learn from incidents to strengthen their security posture for the future.

Unit-05: Wearable Technologies for Q.4

1. What is wearable technology, and what makes it unique?

Wearable technology refers to electronic devices that are worn on the body, such as smartwatches and fitness trackers, designed to integrate seamlessly into daily life. These devices often connect to the internet or other devices to provide users with real-time data, making them valuable for health monitoring, communication, and convenience.

2. What are some common applications of wearable technology?

Wearable technology is widely used in healthcare to monitor vital signs, track physical activity, and manage chronic conditions. It's also applied in sports and fitness, providing performance analytics, as well as in safety, such as wearable devices for tracking employee health in hazardous work environments.

3. What are some challenges to the widespread adoption of wearable technology?

Key challenges include data privacy concerns, as wearables often collect sensitive health information, and limited battery life, which can affect usability. Additionally, device accuracy and the high cost of some advanced wearables can be barriers for users seeking reliable and affordable options.

Name of the Subject: Technology Trends in IT

Course Code: 504 **Semester: I**

4. What types of wearable devices are currently available, and how are they used?

Common wearable devices include smartwatches, fitness trackers, smart glasses, and wearable medical devices. Smartwatches and fitness trackers monitor activity and health metrics, smart glasses provide augmented reality experiences, and wearable medical devices track specific health data, like heart rate and glucose levels. Each device type serves different purposes, from entertainment to health monitoring.

5. How is wearable technology transforming healthcare, and what are its implications?

Wearable technology in healthcare allows for continuous health monitoring, enabling early detection of medical issues and real-time feedback for users and healthcare providers. This transformation supports personalized care and remote patient management, making healthcare more accessible and efficient. As wearables become more advanced, they have the potential to reduce healthcare costs, improve outcomes, and empower users to take control of their health.