1. A cloud storage provider offers a Service Level Agreement (SLA) with 99.95% availability. How much downtime per year does this allow?

1. **~4 hours**
2. ~8 hours
3. ~20 hours
4. ~40 hours

2. A cloud synchronization system uses a block-level sync method where only changed blocks are transmitted. If a file of 1 GB undergoes 5% changes and each block is 4 MB, how many blocks are transmitted?

1. 10 blocks
2. 12 blocks
3. **13 blocks**
4. 15 blocks

3. A cloud storage system has a redundancy factor of 3, meaning data is replicated 3 times. If a company uploads 500 GB, what is the total storage consumed?

1. 500 GB
2. **1,500 GB**
3. 2,000 GB
4. 1,000 GB

4. Which security measure is most effective in preventing unauthorized access to cloud storage?

1. Data compression
2. **Multi-factor authentication (MFA)**
3. Storing data in multiple locations
4. Implementing blockchain for storage

5. Which of the following cloud storage services provides block-level storage?

1. Amazon S3
2. Google Cloud Storage
3. Microsoft Azure Blob Storage
4. **Amazon EBS**

6. A financial institution is using cloud storage for transactional databases. Which characteristic is most critical?

1. High latency tolerance
2. **Immediate consistency**
3. Multi-region replication
4. Data deduplication

7. A cloud service provider offers 99.99% availability for its storage system. How much downtime can be expected per year?

1. **52.56 minutes**
2. 8.76 hours
3. 4.38 hours
4. 5.26 hours

8. Which of the following storage types is best suited for archival data in cloud computing?

1. Block storage
2. **Object storage**
3. File storage
4. RAM-based storage

9. A cloud storage provider offers file-sharing services with a pricing model based on bandwidth usage. If a user shares a 10 GB file with 100 people and each person downloads it twice, assuming a cost of $0.01 per GB transferred, what will be the total cost incurred?

1. $10
2. **$20**
3. $200
4. $100

10. A company backs up 10 TB of data daily to cloud storage with a deduplication ratio of 4:1. How much storage is used per month?

1. 50 TB
2. **75 TB**
3. 100 TB
4. 250 TB

11. A company uses a cloud provider that charges $0.10 per GB for outbound data transfer up to 10 TB, and $0.08 per GB beyond 10 TB. If the company transfers 15 TB of data in a month, what is the total cost?

1. $1,200
2. **$1,400**
3. $1,300
4. $1,500

12. A distributed SQL query runs in a cloud-based data warehouse, scanning 200 million records. After performance tuning using columnar storage and partitioning, the query executes 40% faster. What is the new number of records processed?

1. 120 million
2. 160 million
3. 140 million
4. **100 million**

13. A cloud provider offers three storage tiers: Standard: $0.023 per GB-month Infrequent Access: $0.012 per GB-month Archive: $0.004 per GB-month A company stores 50 TB of data, 20 TB of which can be moved to Archive, and 15 TB to Infrequent Access. What is the optimized monthly cost?

1. $730
2. $880
3. **$650**
4. $920

14. A company runs 4 virtual machines (VMs) in the cloud. Each VM costs $0.25 per hour on an on-demand plan but costs 40% less on a reserved instance plan. What is the monthly savings if the company switches all VMs to reserved instances? (Assume 30 days per month, running 24x7).

1. $1,152
2. $1,440
3. **$960**
4. $1,280

15. A company wants to share sensitive files across multiple devices while ensuring end-to-end encryption. They decide to use Transport Layer Security (TLS) for data in transit and AES-256 encryption for data at rest. Which of the following statements is TRUE regarding this security model?

1. TLS ensures files remain encrypted at rest and in transit.
2. **AES-256 encryption prevents unauthorized access, even if the cloud provider is compromised.**
3. TLS can decrypt files on the server before sending them to clients.
4. AES-256 encryption is only useful when combined with asymmetric encryption.

16. A user wants to share files securely between a smartphone, a tablet, and a laptop. The file-sharing application supports: End-to-end encryption (E2EE) with RSA-2048 and AES-256 TLS 1.3 for secure communication channels Digital signatures for file integrity Which of the following attacks is still possible despite these security measures?

1. Man-in-the-middle (MITM) attack
2. Unauthorized file modification
3. **Private key theft from a compromised device**
4. Data interception in transit

17. A company uses a zero-trust security model and stores files in the cloud. They want to: Ensure only authorized devices access files Prevent data exposure even if cloud servers are breached Enable secure file sharing across multiple devices Which combination of technologies best satisfies these requirements?

1. OAuth 2.0, TLS 1.3, and data obfuscation
2. **Multi-factor authentication (MFA), AES-256 encryption, and client-side encryption**
3. SSL certificates, RSA encryption, and firewall rules
4. VPN tunneling, TLS 1.2, and password-protected ZIP files

18. A multinational company wants to store encrypted files on regional cloud servers located in Europe and the US. The files must remain encrypted in transit and at rest, ensuring compliance with GDPR and US CLOUD Act regulations. Which of the following strategies best ensures compliance and security?

1. **Use TLS 1.3 for transport security and client-side AES-256 encryption before uploading data.**
2. Store unencrypted data on servers and rely on the cloud provider?s security policies.
3. Encrypt data at rest using AES-128 and use TLS 1.2 for secure transmission.
4. Use SHA-256 hashing for file integrity without encryption, ensuring compliance with GDPR.

19. A document collaboration platform allows users to edit shared files across multiple devices. The security model ensures: Transport Security: Files are transferred over TLS 1.3. File Encryption: AES-256 encryption for data at rest. Update Tracking: Each file update is hashed using SHA-512 and stored on a blockchain. Which attack is still possible despite these security measures?

1. Man-in-the-middle (MITM) attack
2. **Unauthorized file modification by a compromised user**
3. Data interception during transmission
4. Server-side encryption key leakage

20. A company encrypts 100 GB of data per day using AES-256 before storing it in the cloud. The cloud provider charges: $0.03 per GB for standard storage $0.01 per GB for retrieval $0.05 per GB for encryption processing What is the total monthly cost of storing, retrieving, and encrypting this data?

1. $1,500
2. $1,800
3. **$1,200**
4. $1,650

21. A company stores its backup data in a multi-region cloud setup. During disaster recovery testing, data retrieval is inconsistent. What factor is most likely causing this issue?

1. Differences in network latency between regions
2. Cloud provider's internal network congestion
3. **Storage replication delay between regions**
4. Failure of load balancing among data centers

22. A cybersecurity team detects unusual activity in their cloud storage logs at 2 AM daily. What is the most efficient approach to identify if this is an APT attack?

1. Block all access during 2 AM to prevent breaches
2. **Analyze behavioral patterns of logins and file accesses**
3. Monitor unusual outbound traffic at the time of activity
4. Change encryption keys regularly

23. A cloud provider offers a choice between AES-256 and RSA-4096 encryption. Which factor should a company consider when choosing between them for large-scale file storage?

1. **Encryption key size vs. processing time**
2. Storage cost per encrypted file
3. Regulatory compliance and audit requirements
4. Ease of key management and recovery

24. A file synchronization service prioritizes newer versions over older ones. A critical document gets overwritten by a less accurate version. What mitigation strategy should be implemented?

1. Implement user access restrictions
2. **Enable version control for file recovery**
3. Use blockchain-based immutable logging
4. Increase logging and monitoring for changes

25. A forensic investigation of a cloud breach reveals a time-stamped log deletion pattern every 6 hours. What inference can be drawn from this pattern?

1. Cloud provider backup system failure
2. Insider threat deleting logs
3. **Automated attack script clearing traces**
4. Accidental deletion by system processes

26. A company experiences a sudden surge in cloud storage costs despite no increase in stored data. What could be the most probable reason?

1. **Increase in API calls for frequent data retrieval**
2. Malware infection causing repeated uploads
3. Shadow IT usage within the organization
4. Unexpected migration of data to premium storage

27. A cloud storage provider implements deduplication to save space. However, users report slow access times. What trade-off does deduplication introduce?

1. Additional encryption layers added
2. Increase in storage redundancy
3. **Compression overhead causing delays**
4. Limited processing power for deduplication handling

28. A user notices that their cloud storage allows access to shared files even after revoking permissions. What is the probable security flaw?

1. Temporary cache retention in the cloud
2. Delayed permission revocation settings
3. **Residual access tokens still valid**
4. Cloud provider security misconfiguration

29. An organization wants to ensure zero-trust security in cloud storage. Which of the following should be the first step in implementing this model?

1. Implement role-based access control (RBAC)
2. Use multi-factor authentication
3. **Limit access based on least privilege**
4. Enforce zero-trust network segmentation

30. A team wants to minimize latency when accessing frequently used cloud files. Which cloud architecture principle should they leverage?

1. Deploying additional encryption layers
2. Using global CDN caching
3. **Leveraging edge computing**
4. Reducing data redundancy

31. A storage system is designed with 500 GB of data. If the system is expected to lose 0.1% of data every year, how much data will be lost in 5 years?

1. **2 GB**
2. 5 GB
3. 0.5 GB
4. 50 GB

32. A cloud service offers 99.9% uptime. What is the downtime allowed in a 30-day month?

1. 1 hour
2. **43 minutes**
3. 72 minutes
4. 50 minutes

33. A system has a redundancy factor of 4. If the data size is 1 TB, how much storage is required to ensure redundancy?

1. 1 TB
2. 2 TB
3. 3 TB
4. **4 TB**

34. In a cloud storage system, data loss is 0.05% per year. How much data would be lost from a 200 GB system in 2 years?

1. **0.2 GB**
2. 0.1 GB
3. 0.05 GB
4. 1 GB

35. A system has 20 users, each of whom can have 5 roles. How many role combinations are possible?

1. **100**
2. 125
3. 50
4. 200

36. An IAM system allows 62 characters (26 lowercase, 26 uppercase, 10 digits). How many possible passwords of length 6 can be created?

1. 5,68,00,235
2. 5,68,00,000
3. 56,80,00,00,000
4. **62^6**

37. If a user has 3 types of access levels (admin, user, guest) and can access 10 resources, how many different access control policies can be created?

1. **30**
2. 100
3. 1000
4. 300

38. An IAM system uses multi-factor authentication (MFA). If each user has 3 passwords, 4 security questions, and 5 fingerprints, how many combinations of authentication can be created?

1. 20
2. **60**
3. 240
4. 180

39. A cloud service guarantees 99.95% uptime. How much downtime is acceptable in a month?

1. **20 minutes**
2. 43.2 minutes
3. 36 minutes
4. 100 minutes

40. If the cloud provider has 10 regions and the system distributes the load equally among them, how much of the total system capacity does each region handle?

1. 1%
2. 5%
3. **10%**
4. 12%

41. A cloud storage provider offers two encryption options: AES-128 and AES-256. If the time to brute-force AES-128 is 2?? years, what is the approximate time required to brute-force AES-256, assuming ideal conditions?

1. 2?? years
2. 2?? years
3. **2??? years**
4. 2??? Years

42. A file of size 500 MB is encrypted using AES-256 before uploading to the cloud. The encryption process takes 2 milliseconds per MB. How much time will the encryption take for the entire file?

1. **1 second**
2. 2 seconds
3. 5 seconds
4. 10 seconds

43. A user wants to encrypt 1 GB of data before storing it in the cloud. The symmetric encryption method takes 0.5 ms per MB, while an asymmetric encryption method takes 10 ms per MB. What is the time difference between the two methods for encrypting the entire file?

1. **9.5 seconds**
2. 5 seconds
3. 9500 milliseconds
4. 50 seconds

44. A company wants to store sensitive customer data in the cloud. It has three options: Provider A (AES-256, multi-location replication, Zero-Knowledge Proof), Provider B (AES-128, lower cost, does not store encryption keys), Provider C (No encryption, high speed). Which provider should they choose based on security considerations?

1. **Provider A**
2. Provider B
3. Provider C
4. Any provider, as encryption is not a concern

45. A user encrypts files before uploading them to cloud storage. They store the encryption key in the same cloud storage. What is the biggest security risk in this approach?

1. Increased encryption processing time
2. **The encryption key can be compromised if the cloud provider is breached**
3. The encryption strength is reduced
4. The key will require frequent updates

46. RSA encryption requires generating two large prime numbers p and q to compute n = p ? q. If p and q each have 1024 bits, what is the approximate number of bits in n?

1. 1024 bits
2. **2048 bits**
3. 4096 bits
4. 512 bits

47. A system uses a 128-bit encryption key. An attacker can test 10?? keys per second. How long would it take (in years) to try all possible keys in a worst-case scenario?

1. 10? years
2. 10? years
3. **10?? years**
4. 10?? years

48. A system uses a hybrid encryption approach where a 2048-bit RSA key is used to encrypt an AES-256 session key, which then encrypts a 2 GB file. Given that AES encryption speed is 100 MB/s and RSA encryption speed is 5 MB/s, how much total time will it take to encrypt the file?

1. 10 seconds
2. **20 seconds**
3. 25 seconds
4. 30 seconds

49. A 500 MB file is hashed using SHA-256, and the resulting hash is stored separately. Later, the file is downloaded, and its hash is recomputed. If only 1 bit of the file is altered, what is the probability that the hash remains unchanged?

1. **0**
2. 50%
3. 1 in 2???
4. 1 in 2???

50. A user encrypts a 100 MB file with AES-256 and stores the encrypted file in the cloud. The encryption key is stored in a separate cloud service. What is the biggest risk of this approach?

1. **The encryption key can be compromised if the second service is breached**
2. AES-256 encryption is weak
3. The file can still be decrypted without the key
4. The key will require frequent updates

1. A user takes 1.2 seconds to point and click on a button. How much time is required for 250 clicks?

1. 4 minutes
2. **5 minutes**
3. 6 minutes
4. 7 minutes

2. A positioning device has a 95% accuracy rate. If 2,000 actions are performed, how many are incorrect?

1. 50
2. 75
3. **100**
4. 120

3. A user interface requires 3 steps to complete a task. If 500 tasks are completed, how many steps are taken in total?

1. 1200
2. 1400
3. **1500**
4. 1600

4. A user types at 80 words per minute. How long will it take to type 2,400 words?

1. 20 minutes
2. 25 minutes
3. **30 minutes**
4. 35 minutes

5. A VR system refreshes its display every 10 milliseconds. How many refreshes occur in one second?

1. 50
2. 75
3. **100**
4. 120

6. A user recalls 60% of the content from a training module. If the module has 250 points, how many are recalled?

1. 140
2. **150**
3. 160
4. 170

7. A display system operates at 144 Hz. How many frames are shown in a 5-minute session?

1. 36000
2. 40000
3. **43200**
4. 45000

8. A WIMP interface reduces errors by 20%. If the initial error rate was 500 per week, what is the new error rate?

1. 350
2. 375
3. **400**
4. 425

9. A multimodal interface receives 6 user interactions per second. How many interactions occur in 4 hours?

1. 80000
2. 81500
3. 83000
4. **86400**

10. A text entry system allows 10 keystrokes per second. How many keystrokes occur in 30 minutes?

1. 15000
2. 16000
3. 17000
4. **18000**

11. Which of the following is a key principle of Interaction Design?

1. Reducing user involvement;
2. Prioritizing system functionality over usability;
3. **User-centered approach;**
4. Increasing complexity for expert users;

12. A well-designed navigation system should:

1. Require users to memorize paths;
2. **Allow easy and intuitive movement;**
3. Be hidden to reduce clutter;
4. Focus only on aesthetics;

13. Which of the following best describes scenarios in interaction design?

1. Code-level design patterns;
2. **User stories describing interactions;**
3. Algorithmic flowcharts;
4. Network protocols;

14. What is the primary objective of screen design and layout?

1. To ensure an aesthetically pleasing interface only;
2. **To enhance usability and efficiency;**
3. To make the UI as complex as possible;
4. To minimize user engagement;

15. The HCI life cycle model primarily focuses on:

1. Software development speed;
2. **Continuous user feedback and iteration;**
3. Maximizing code reusability;
4. Minimizing front-end design;

16. Which usability engineering phase deals with user testing?

1. Requirements gathering;
2. Implementation;
3. Evaluation;
4. **Coding;**

17. Interactive design emphasizes:

1. **System responsiveness;**
2. Only hardware compatibility;
3. Code optimization techniques;
4. Machine learning algorithms;

18. Prototyping in interactive design is used to:

1. Improve software runtime performance;
2. **Test and refine usability aspects;**
3. Reduce network latency;
4. Optimize backend databases;

19. Which of the following is a usability principle?

1. **Flexibility;**
2. Unpredictability;
3. Complexity;
4. Hidden user feedback;

20. What do design standards in HCI ensure?

1. **Better usability and consistency;**
2. More complex user interactions;
3. Longer software development time;
4. Higher processing power;

21. A user interface management system processes 120 user actions per minute. If each action takes 0.5 seconds to execute, how much total execution time is required for 120 actions?

30 seconds

45 seconds

**60 seconds**

75 seconds

22. A windowing system allows a user to open 4 applications simultaneously. If each application consumes 250 MB of RAM, what is the total memory consumed?

1. 500 MB
2. 750 MB
3. **1000 MB**
4. 1250 MB

23. A cognitive model predicts that a user takes 3 seconds to process each step in a task. If a task consists of 20 steps, what is the total time taken to complete the task?

1. 40 seconds
2. 50 seconds
3. **60 seconds**
4. 70 seconds

24. An evaluation method requires 5 experts to analyze a user interface. Each expert takes 45 minutes to complete the analysis. What is the total time spent by all experts?

1. 150 minutes
2. 200 minutes
3. **225 minutes**
4. 250 minutes

25. A help system provides adaptive support by analyzing user behavior every 15 minutes. If a user works for 2 hours, how many analyses will be performed?

1. 6
2. **8**
3. 10
4. 12

26. A multimodal interface receives 200 voice inputs and 300 text inputs in an hour. What is the total number of inputs received?

1. 400
2. 450
3. **500**
4. 600

27. A user support system receives an average of 90 help requests per day. If the system operates for 30 days, how many requests does it handle in total?

1. 2000
2. 2400
3. **2700**
4. 3000

28. A user spends an average of 10 minutes per session using a windowing system. If they use it 5 times a day, what is the total time spent in a week?

1. 200 minutes
2. 300 minutes
3. **350 minutes**
4. 400 minutes

29. A touch-based multimodal interface processes 150 gestures per hour. If a user interacts for 3 hours, how many gestures are processed?

1. 300
2. 400
3. **450**
4. 500

30. An adaptive help system reduces task completion time by 20%. If a task originally takes 50 minutes, how much time does it take after adaptation?

1. 30 minutes
2. 35 minutes
3. **40 minutes**
4. 45 minutes

31. A user takes 1.8 seconds to process each step in a 25-step task. What is the total time required?

1. 30 seconds
2. 35 seconds
3. 40 seconds
4. **45 seconds**

32. A collaboration system reduces communication delays by 20%. If the initial delay was 50 seconds, what is the new delay?

1. 30 seconds
2. 35 seconds
3. **40 seconds**
4. 45 seconds

33. A linguistic model processes 5 sentences per second. How many sentences will it process in 15 minutes?

1. 3000
2. 4000
3. **4500**
4. 5000

34. A knowledge-based system has a 92% accuracy rate. If it processes 1,500 queries, how many are incorrect?

1. 100
2. **120**
3. 150
4. 180

35. A task analysis system improves efficiency by 15%. If the initial task completion time was 200 minutes, what is the new time?

1. 160 minutes
2. **170 minutes**
3. 180 minutes
4. 190 minutes

36. A physical model predicts that a user takes 3 seconds to adjust a device setting. How many adjustments occur in 10 minutes?

1. 150
2. 175
3. **200**
4. 225

37. A face-to-face communication system reduces misunderstanding by 30%. If the initial error rate was 500 misunderstandings per month, what is the new rate?

1. 300
2. **350**
3. 375
4. 400

38. A conversation model predicts that a user speaks 120 words per minute. How many words will be spoken in a 45-minute meeting?

1. 4500
2. 5000
3. **5400**
4. 5800

39. A collaborative system reduces task completion time by 25%. If the initial time was 80 minutes, what is the new time?

1. 55 minutes
2. **60 minutes**
3. 65 minutes
4. 70 minutes

40. A group working model increases efficiency by 10%. If the original output was 1,200 tasks per week, what is the new output?

1. 1250
2. 1300
3. **1320**
4. 1400

41. Ubiquitous computing enhances the seamless integration of digital and physical environments. What is a logical conclusion based on this?

1. **Ubiquitous computing allows digital interactions to occur naturally in daily activities.**
2. Ubiquitous computing eliminates the need for the internet.
3. Ubiquitous computing reduces the usability of smart devices.
4. Ubiquitous computing is only beneficial in industrial applications.

42. Virtual reality (VR) provides an immersive digital experience. What is a logical conclusion based on this?

1. **Virtual reality enhances user engagement by simulating real-world environments.**
2. Virtual reality is only useful for entertainment purposes.
3. Virtual reality does not contribute to skill development.
4. Virtual reality makes physical training obsolete.

43. Augmented reality (AR) overlays digital information onto the real world. What is a logical conclusion based on this?

1. **Augmented reality enhances real-world interactions by providing additional information.**
2. Augmented reality completely replaces physical environments.
3. Augmented reality requires no hardware to function.
4. Augmented reality reduces the effectiveness of user engagement.

44. Information visualization simplifies complex datasets. What is a logical conclusion based on this?

1. **Information visualization improves data interpretation and decision-making.**
2. Information visualization is only applicable in academic research.
3. Information visualization increases the complexity of understanding data.
4. Information visualization replaces data analytics tools.

45. Hypertext allows non-linear navigation of digital content. What is a logical conclusion based on this?

1. **Hypertext enables users to access information in a flexible manner.**
2. Hypertext forces users to follow a fixed path.
3. Hypertext reduces accessibility of digital content.
4. Hypertext eliminates the need for structured web content.

46. The World Wide Web (WWW) enables global information sharing. What is a logical conclusion based on this?

1. **The WWW allows users to access and share information worldwide.**
2. The WWW is limited to local networks.
3. The WWW eliminates the need for search engines.
4. The WWW prevents real-time communication.

47. Static web content remains unchanged unless manually updated. What is a logical conclusion based on this?

1. **Static web pages provide consistent information without requiring frequent updates.**
2. Static web pages automatically update based on user interactions.
3. Static web pages require a database for content storage.
4. Static web pages support interactive user engagement.

48. Dynamic web content updates based on user interactions or data retrieval. What is a logical conclusion based on this?

1. **Dynamic web content enhances user engagement by providing real-time updates.**
2. Dynamic web content remains unchanged after creation.
3. Dynamic web content does not require backend processing.
4. Dynamic web content reduces personalization options.

49. Groupware systems facilitate collaborative work among multiple users. What is a logical conclusion based on this?

1. **Groupware systems improve teamwork by enabling real-time collaboration.**
2. Groupware systems limit user interaction.
3. Groupware systems only support document sharing.
4. Groupware systems do not enhance communication.

50. Decision Support Systems (DSS) assist in analyzing data for decision-making. What is a logical conclusion based on this?

1. **DSS enhances business intelligence by providing data-driven insights.**
2. DSS replaces human decision-making entirely.
3. DSS is only applicable in financial organizations.
4. DSS eliminates the need for data visualization.

1.A cloud data center has 500 servers, each with a storage capacity of 2TB If each server is utilized at 70% capacity, what is the total utilized storage in the data center?

A) 500 TB

**B) 700 TB**

C) 1000 TB

D) 1400 TB

2.A distributed cloud storage system stores data in blocks of 512MB across multiple nodes. If a (CO1) file of 20GB needs to be stored, how many nodes are required assuming even distribution?

A) 20

**B) 40**

C) 50

D) 80

3.In a cloud storage system, data retrieval latency follows a hierarchical structure with main (COI) memory access taking 10ns, SSD access taking 100µs, and HDD access taking 10ms. If a cloud system has an 80% cache hit rate in main memory and 15% in SSD, what is the expected access latency?

**A) 1.5 ms**

B) 2 ms

C) 3.5 ms

D) 5 ms

4.A cloud storage provider uses RAID-5 for data protection across 6 disks, each with 4TB (C01) capacity. How much total usable storage is available after parity storage allocation?

A) 16 TB

**B) 20 TB**

C) 24 TB

D) 32 TB

5.A cloud-based backup system writes data at a rate of 500MB/s. If the system needs to back 2TB of data, how long will the backup process take?

A) 2000

B) 3000s

**C) 4000s**

D) 5000s

6.A file stored in a cloud storage service has a replication factor of 3 and a chunk size of 256MB.If the file is 10GB in size, how much total storage space does it occupy?

A) 10GB

B) 20GB

**C) 30GB**

D) 40GB

7.A cloud system follows an erasure coding technique where a 10GB file is split into 5 data blocks and 2 parity blocks. How much total storage space is required?

A) 10GB

B) 12GB

**C) 14GB**

D) 16GB

8.A cloud storage system uses deduplication, reducing the original data size from 5TB to 3TB. If the average file size before deduplication was 10MB, how many files were removed?

A) 100,000

**B) 200,000**

C) 300,000

D) 400,000

9.A cloud computing system distributes data across multiple data centers. If a request is equally likely to be served from any of 4 data centers and each center has a 99.5% availability, what is the probability that the request is served successfully?

A) 0.980

B) 0.995

**C) 0.999**

D) 1.000

10.A cloud storage provider offers data redundancy by using a mirroring technique. If a 100TB. dataset is stored using 2x mirroring, what is the total storage required?

A) 100TB

**B) 200TB**

C) 300TB

D) 400TB

11.What is the primary function of cloud storage?

A) To provide unlimited internet access

**B) To store and manage data on remote servers**

C) To enhance processing speed of computers

D) To replace RAM in computers

12.Which of the following is NOT a key advantage of cloud storage?

A) Accessibility from anywhere

B) Scalability

**C) High maintenance costs for users**

D) Automatic backups

13.Which of the following companies offers cloud storage services?

**A) Dropbox**

B) Fastagram

C) Netflix

D) WhatsApp

14.Which is NOT a feature of cloud storage services?

A) Data encryption

B) Pay-as-you-go pricing model

**C) Physical proximity to the stored data**

D) Integration with multiple devices

15.Cloud storage is commonly used for.

A) Video editing in offline mode

**B) Data backup and recovery**

C) Increasing RAM performance

D) Reducing the speed of internet browsing

16.Why is Transport Layer Security (TLS) important in cloud storage?

A) It speeds up the file upload process

**B) It prevents unauthorized access during data transmission**

C) It compresses large files before sending them

D) It removes duplicate files from cloud storage

17.Which cloud storage interface allows users to interact with files using a graphical representation via the web?

A) Command-line Interface

**B) Browser Interface**

C) File Transfer Protocol (FTP)

D) Direct Memory Access (DMA)

18.How does file-sharing security impact cloud storage users?

A) It prevents any modifications to shared files.

B) It allows files to be accessed without any authentication

**C) It ensures that only authorized users can view or modify shared data**

D) It restricts access to files based on file size

19.Which security requirement ensures that cloud-stored data remains intact and unaltered?

A) Availability

**B) Integrity**

C)Confidentiality

D)Authentication

20.Which of the following is an advantage of cloud storage from a user's perspective?

A) Data can only be accessed from a single device

B) Storage capacity is limited to local hardware

**C)Data is accessible from multiple devices anywhere**

D) Cloud storage does not require an internet connection

22.A cloud storage system supports data encoding it store the changes. If a 10B undergoes 100 changes of 2MB each, what is the total storage required?

**A) 10GB**

B) 12GB

C) 1.5GB

D) 2GB

23.A cloud security system uses TLS encryption with a 2048-bit key. If each encryption operation takes Sass, how much time is required to encrypt 1000 requests in parallel across 10 servers?

B) 18

**C) 0.5**

D) 10

24.A distributed cloud storage system stores data across multiple nodes. If a file of 50GB is split into 512MB chunks and stored redundantly across 3 nodes, how many total chunks are generated?

A) 100

B) 150

**C) 300**

25.A user uploads a 5GB file to a cloud storage service using a browser interface. If the system uses a block size of 256MB, how many blocks are created?

A)5

B) 10

**C) 20**

D) 40

26.A cloud security framework requires multi-factor authentication for 500 users. If authentication time per user is 3 seconds, how long will it take for all users to complete authentication in a system handling 50 concurrent authentications?

A) 10s

**B) 30s**

C) 60s

D) 100s

27.A cloud storage system uses RAID-6 for redundancy across 8 disks, each with a capacity of 2TB. How much total usable storage is available after parity allocation?

A) 8TB

B) 10TB

**C) 12TB**

D) 14TB

28.A cloud system encrypts user files using AES-256. If encryption takes 4ms per MB, how long does it take to encrypt a 10GB file?

**A) 40s**

B) 80s

C) 120s

D)100s

29.A cloud system with deduplication reduces bandwidth usage by removing 30% of redundant (CO2) data. If the original transmission size was 211TB, what is the new transmission size?

A)106TB

B) 1.4TB

**C)147TB**

D) 15TB

30.A cloud storage provider uses compression to optimize storage. If a 20GB file is compressed with a 5:1 ratio, what is the final storage size?

A) 2GB

**B) 4GB**

C) 5GB

D) 10GB

31.A cloud storage provider implements a zero-trust model requiring multi-factor authentication (MFA), If each authentication step takes 2 seconds and a user must complete 3 steps, how long does the entire authentication process take?

A) 4s

B) 5s

**C) 6s**

D)3s

32.An Advanced Persistent Threat (APT) infiltrates a cloud storage system and exfiltrates 1MB of data every 5 minutes. How much data is stolen in a day?

**A) 288MB**

B) 500MB

C) 1GB

D) 2GB

33.A cloud storage forensic team detects an anomaly where timestamps of log files are manipulated to evade detection. If each log file update takes 200ms and an attacker modifies 500 log files, how long does the attack take?

A) 10s

B) 20s

C) 30s

**D) 50s**

* Files modified = 500
* Time per file update = 200ms = 0.2s
* Total time =
* **500×0.2=100s**
* **500×0.2=100*s***

34.A cloud provider uses an asymmetric encryption scheme for authentication. If encryption takes 50ms and decryption takes 80ms per authentication request, how long does it take to process 1,000 authentication requests in parallel over 10 servers?

A) 5s

B) 8s

C) 10s

**D) 12s**

* Encryption time per request = 50ms
* Decryption time per request = 80ms
* Total time per request =
* **50ms+80ms=130ms**
* **50*ms*+80*ms*=130*ms***
* Total requests = 1000
* Servers = 10
* Time required =
* **1000×130ms10=13000ms=13s**
* **10**
* **1000×130*ms***
* **​**
* **=13000*ms*=13*s***

35.A security audit on a cloud storage system shows that 20% of files have been accessed by unauthorized users. If the system contains 500,000 files, how many files were compromised?

A) 50,000

B) 75,000

**C) 100,000**

D) 150,000

36.A cloud backup service performs full backups weekly and incremental backups daily. If a filt backup requires 1TB and sach incremental backup requires 100GB, what is the total storage

A) 4TB

B) 5TB

**C) 6TB**

D) 7TB

37.A distributed cloud storage system has 8 nodes, and each node stores 2TB of data with 3x replication. What is the total effective storage available?

**A) 5.33TB**

B) 6TB

C)5TB

D) 10TB

38.A forensic investigator finds that a cloud storage system generates a log entry every 250ms for security monitoring. How many log entries are generated in one hour?

A) 10,000

B) 12,500

**C) 14,400**

D) 20,000

39.A side-channel attack exploits timing variations in a cloud encryption algorithm. If an attacker needs 1,000 samples with a Sms delay each to extract a key, how long does the attack take?

A) 2.5s

**B) 5s**

C) 10s

D) 15s

40.A cloud analysis tool checks for integrity violations every 15 minutes across 50,000 files. If each check takes Ims per file, how long does each integrity check cycle take"

A) 208

B) 30s

**C) 50s**

D) 60s

41.Which is a drawback of client-side encryption in cloud storage?

A) Higher risk of data breaches

**B) Increased encryption key management complexity**

C) Reduced data availability

D) Incompatibility with HTTPS protocols

42.Which cloud storage service was discontinued by Ubuntu?

A) CloudMe

**B) UbuntuOne**

C) Mozy

D) Whula

43.Which type of security threat exploits time-related vulnerabilities in cloud storage?

A) Phishing

**B) Time-based side-channel attacks**

C) SQL Injection

D) Brute force attack

44.encryption technique ensures data security in cloud client-server communication?

A) Symmetric encryption

**B) Asymmetric encryption**

C) Plaintext storage

D) Stenography

45.Which cloud storage provider is best known for its real-time file synchronization?

A) CloudMe

B) Crash Plan

**C) Dropbox**

D) Mozy

46.What is the primary concern in time-related cloud security attacks?

A) Encryption key storage

**B) Data synchronization delays**

C) Unauthorized data replication

D) System load balancing

47.Which security measure is crucial to mitigate persistent threats in cloud storage?

A) Frequent password resets

**B) Implementing zero-trust security models**

C) Enabling file compression

D) Increasing storage capacity

48.What is the first step in analyzing cloud storage devices?

**A) Data extraction**

B) Product selection

C) Security auditing

D) Threat modeling

49.What is a key characteristic of an Advanced Persistent Threat (APT)?

A) A short-term attack with immediate damage

**B) A targeted, long-term cyber attack with stealthy infiltration**

C) A brute force attack on a cloud storage system

D) A denial-of-service (DoS) attack on cloud servers

50.Which of the following is NOT considered an advanced persistent threat (APT) technique?

A) Social engineering

B) Data exfiltration

C)Session hijacking

**D) File compression**