St. MARTIN'S ENGINEERING COLLEGE

(UGC Autonomous)
ESTD : 2002, NAAC (A+) & NBA Accredited, Affiliated to JNTUH,
Approved by AICTE, NIRF & ARIIA Ranked, A Non Minority Institution
Dhulapally, Near Kompally, Secunderabad - 500 100, T.S.

ASSIGNMENT ANSWER BOOKLET

Hall Ticket No. : 2 2 K 8 1 A 0 5 9 9

Name of the Student: Kunal chaudhary

Course : B.tech

Branch : CSE

Year : I/II/III/IV

Sem : I / II

Assignment : I / II

Subject Name : Cloud Computing

Last Date of Submission: 10/11/25

Actual Date of Submission : 10/11/25

MARKS AWARDED

Q.No.	a	b	Total
1			
2			
3			
4			
5			
Total			

Signature of the Student

Signature of the Evaluator

Start Writing from Here

1) Explain the concept of cloud Haskell & compare it with mapreduce.

=> Cloud Haskell is a distributed programming framework for a Haskell programming language. It enables developers to build parallel & distributed applications in a purely functional style, inspired by Erlang's concurrency model.

Key concepts:-

1- Pure Functional programming

2- Message Passing

3- Location Transparency

4- Process Management

5- fault Tolerance

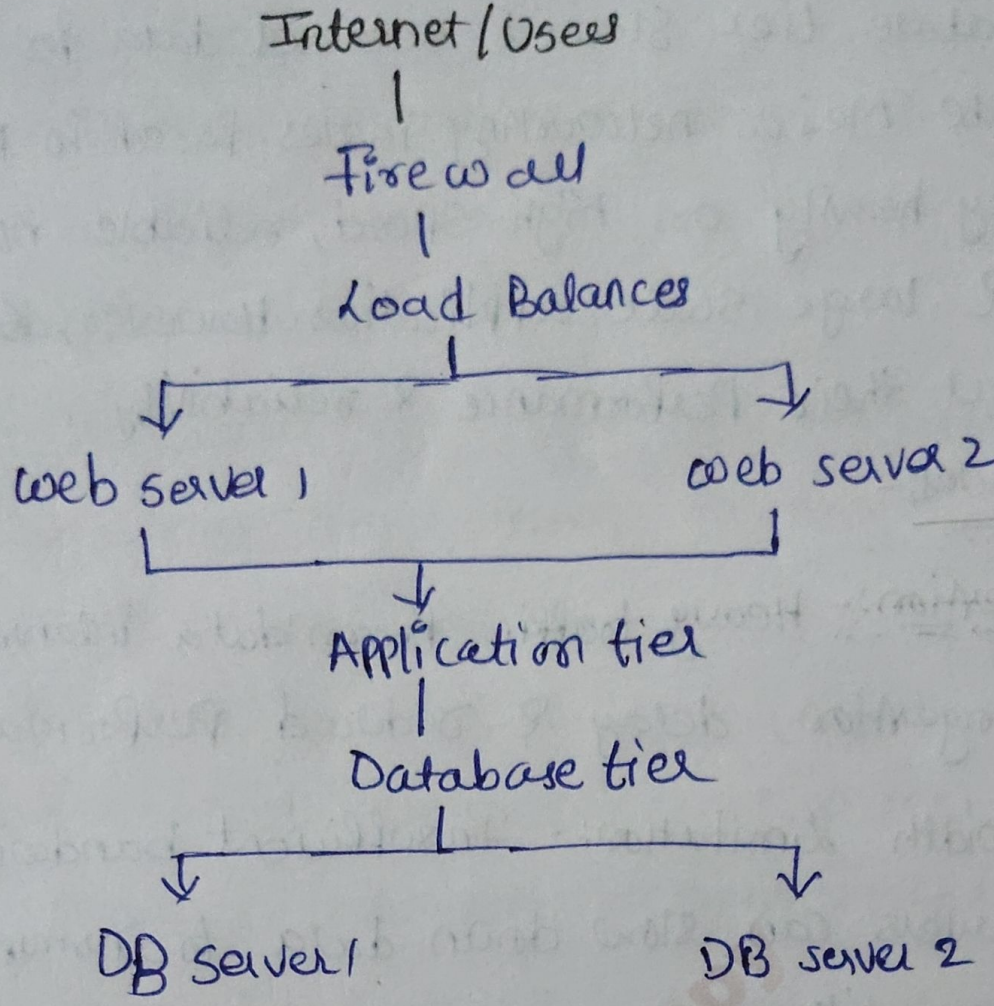
Architecture overview :-

- Nodes :- Machines participating in computation.
- Processes :- Independent units of computation running on nodes.
- Message :- Data sent asynchronously b/w processes.
- Transport Layer :- Handles communication b/w nodes over the network.

Feature	Cloud Haskell	MapReduce
Programming Model	~~Actor~~ model with message passing & Concurrency	Functional model with map & Reduce operations.
Language Base	Implemented in Haskell	Framework (e.g Hadoop) & supports Java, Python.
Execution Model	Dynamic & continuous communication	Batch oriented Processing Model :
Scalability	Highly scalable	Scalable but focused on data Parallelism
DataFlow	Asynchronous message passing	map → shuffle → Reduce stages.

2) Describe the architecture of a Data Center used in Cloud computing.

⇒ A "Data Center" is the backbone of cloud computing - It is a centralized facility that houses computing resources such as Servers, storage system, networking equipment & other components necessary to deliver cloud services efficiently & security. The architecture of a data center is designed to ensure high availability, scalability & reliability for cloud based application & services.



★ Key Layers:-

1. Physical Layer:- This layer includes the Physical infrastructure such as servers, storage devices, cooling systems & power supplies. It provides the hardware foundation for cloud operations.
2. Virtualization layer:- This layers abstracts Physical hardware into virtual resources using hypervisors & virtualization software.
3. Storage Layer:- This layer manage the data storage infrastructure include SAN.
4. Network Layer:- The n/w layer interconnection servers, storage & external networks.

Working:-

1) The internet/users access the system through a firewall for security.
2) Nc Load Balance distributes requests across multiple web servies.
3) The web tier connects to the Application tier, which handles buiness logic.

• The Database tier stores & retrieves data for applications.

3) Discuss the major networking issues faced in Data centres.

⇒ Data centres rely heavily on high-speed, reliable n/w to support cloud computing & large-scale applications. However, several networking issues can affect their performance & reliability.

Key Networking issues:-

1. Networking congestion:- Heavy traffic from data-intensive applications can lead to congestion, delay & reduced performance.
2. Latency & Bandwidth limitation:- Insufficient bandwidth or high latency b/w servers can slow down data transmission & affect cloud service quality.
3. Scalability challenges:- As data centers grow, managing large numbers of switches, routers & connections becomes complex.
4. Load Balancing:- Uneven traffic distribution across servers can overload some resources while others remain underutilized.
5. Energy consumption:- High speed networking equipment consumes significant power impacting operational costs & sustainability.
6. Fault Tolerance & Reliability:- Network failure or link outages can disrupt services, requiring redundancy & failover mechanism.

4) Explain transport layer issues in Data center Networks (DCNs):-

⇒ The transport layer in Data center Network (DCNs) is responsible for reliable data delivery, flow control & congestion management b/w servers. However due to the large scale & dynamic nature of DCNs several issues arise at this layer.

Transport layer issues:-

1. TCP Incast Problem:- Occurs when multiple servers send data simultaneously to a single receiver, causing packet loss & high latency due to buffer overflow at switches.
2. Congestion Control:- Traditional TCP Algorithms are not well suited for DCNs as they may react slowly to congestion, leading to poor utilization & performance drops.
3. Out-of-order packet delivery:- Equal-cost-multi-path (ECMP) routing in DCNs may send packets along different paths, causing packets to arrive out of order & increasing retransmissions.
4. Buffer bloat:- Excessive buffering in switches causes high latency & jitter, degrading performance of real time applications.
5. Inadequate Multipath Support:- Standard TCP does not efficiently utilize multiple available network paths, resulting in optimal throughput.

Fairness & Flow Completion Time:- TCP may not ensure fair bandwidth sharing among flow leading to long completion times for short flow (mice flows) compared to large ones (elephant flow).

Transport layer protocols like TCP face challenge in DCNs due to high traffic Parallelism low latency demands & dynamic workloads.

5a) Explain different security challenges in cloud computing.

⇒ Cloud computing offers flexibility, scalability & cost efficiency but it also introduces several security challenges due to data storage, multi-latency & remote access features.

Security challenges:-

1. Data Breaches:- Unauthorized access or expose of sensitivity data stored in cloud can lead to financial & reputational loses.

2. Data loss:- Accidental deletion, hardcoare failure or malicious attacks may cause permanent data loss if proper backups are not maintained.

3. Insecure APIs:- Cloud services rely on APIs for communication weak or poorly designed. APIs can be exploited by attacks.

4. Account Hijacking:- Attacker can gain control over user accounts through phishing stolen credentials or weak password.

5) Denial of service (DOS) attacks:- overloading cloud several with excessive traffic can distrupt services & degrade performance.

6) Data Privacy & compliance issues:- storage data in different region may violate local privacy laws & regulations like GDPR.

5) b) Discuss advanced Security Mechanisms used to Protect data & applications in the cloud.

⇒ As cloud computing grow, ensuring the Security of data & applications has became a top priority to safeguard information & maintain user trust, cloud Providers & organizations are several advanced Security mechanisms.

1. Data Encryption:- Data is encrypted both at rest (while stored) & in transmit (while being transmitted).
Strong encryption algorithms like AES at rest (while stored) & used.

2. Identity & Access Management (IAM):- IAM ensures that only authorized users can access specific cloud resources.
It uses role-based access control (RBAC), multifactor Authentication (MFA) & single sign on (SSO) to enhance Security.

3. Intrusion Detection & Prevention Systems (IDPs):- Monitors cloud traffic in real time to detect & block malicious activities or attack.

4) Cloud Access Security Broker (CASB):- CASB acts as a security layer b/w users & cloud servies.
They enforce Security Policies, monitor data usage & ensure compliance with regulations.

5) Blockchain Based Security:. Blockchain ensures data integrity transparency, & tamper resistance by maintaining distributed immutable records.

→ Advanced cloud Security Mechanisms such as encryption, IAM zero trust & AI-driven monitoring play a crucial role in Protecting cloud data & applications.