SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB504 DATABASE MANAGEMENT SYSTEMS

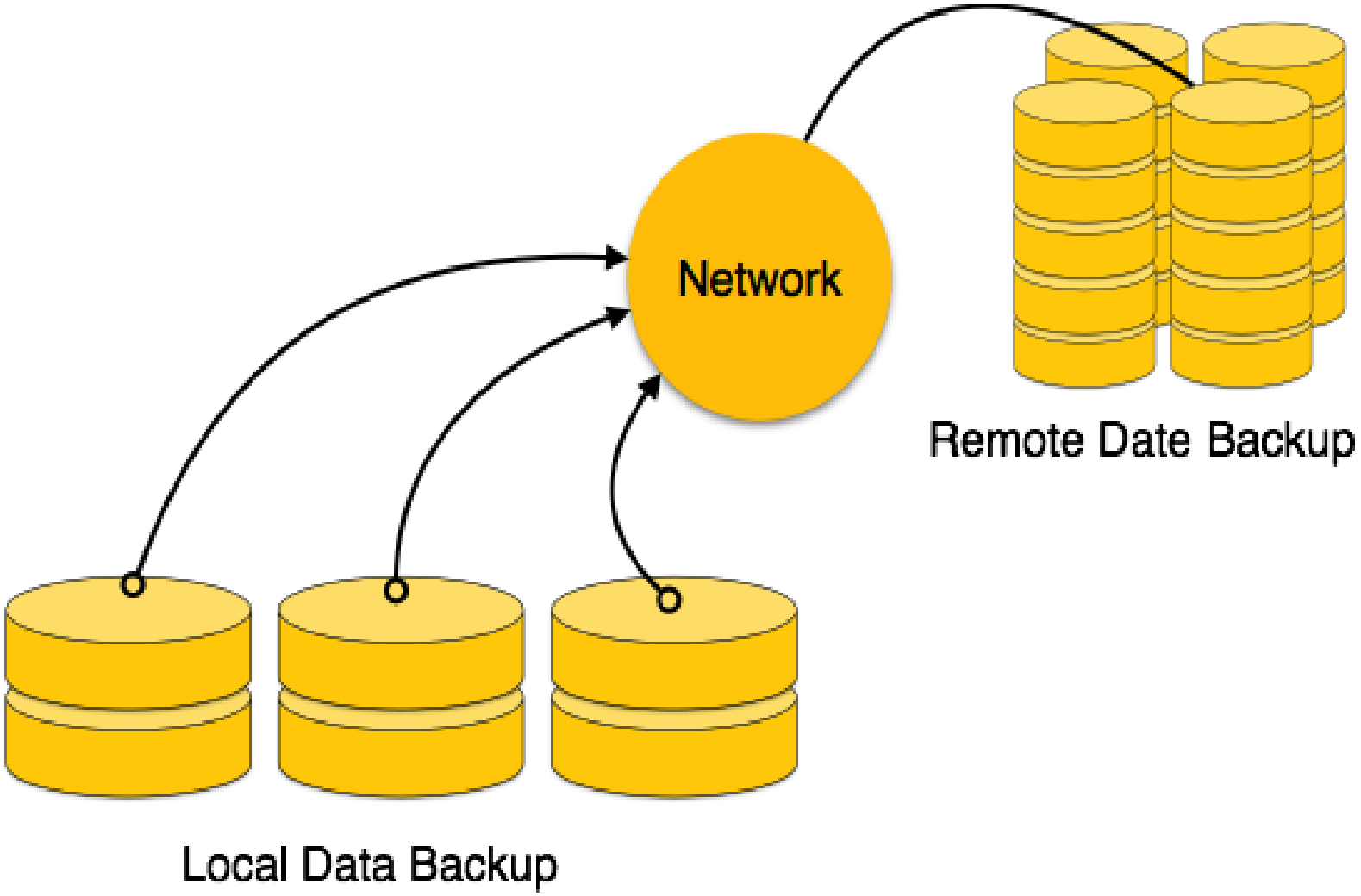
III YEAR / V SEMESTER

Unit V- CONCURRENCY CONTROL AND RECOVERY SYSTEM

Topic : **REMOTE BACKUP SYSTEMS**

Objective:

- ✓ Remote backup provides a sense of security in case the primary location where the database is located gets destroyed.
- ✓ Remote backup can be offline or real-time or online. In case it is offline, it is maintained manually.


Network
Remote Date Backup
Local Data Backup

- ✓ Online backup systems are more real-time and lifesavers for database administrators and investors.
- ✓ An online backup system is a mechanism where every bit of the real-time data is backed up simultaneously at two distant places.
- ✓ One of them is directly connected to the system and the other one is kept at a remote place as backup.

Here are key considerations and techniques for implementing remote recovery systems in DBMS:

1. Data Replication
2. Automated Recovery Processes
3. Point-in-Time Recovery
4. Cloud-Based Recovery
5. Warm Standby and Hot Standby Systems
6. Backup Encryption and Security Measures
7. Load Balancing and Failover
8. Testing and Simulation
9. Monitoring and Alerting
10. Documentation
11. Regulatory Compliance

1. Data Replication:

Synchronous Replication: Real-time replication of data to a remote location ensures that the backup is always up-to-date. However, this may introduce latency in write operations.

Asynchronous Replication: Data is replicated to a remote location with a delay, reducing the impact on primary system performance.

2. Automated Recovery Processes:

Scripted Recovery Procedures: Automate the recovery process using scripted procedures to ensure consistency and reduce the time required for recovery.

3. Point-in-Time Recovery:

Log Shipping: Transmitting transaction logs to a remote location enables point-in-time recovery, allowing the database to be restored to a specific moment in time.

4. Cloud-Based Recovery:

Cloud-Based Disaster Recovery Services:

Cloud providers offer disaster recovery services that allow for the seamless recovery of databases in the cloud in case of a failure at the primary data center.

5.Warm Standby and Hot Standby Systems:

Warm Standby: Maintain a partially synchronized copy of the database at the remote location, reducing the time needed to bring the standby system online.

Hot Standby: Keep a fully synchronized, readily available copy of the database at the remote location for immediate failover.

6.Backup Encryption and Security Measures:

Secure Data Transmission: Ensure that data transmission between the primary and remote locations is secure, especially when dealing with sensitive information.

Access Controls: Implement stringent access controls to prevent unauthorized access to the recovery systems.

7. Load Balancing and Failover:

Automatic Failover: Implement mechanisms for automatic failover to the remote recovery system when the primary system experiences a failure.

Load Balancing: Distribute the workload between the primary and remote systems to ensure optimal performance during normal operation and recovery.

8. Testing and Simulation:

Disaster Recovery Testing: Regularly test the remote recovery systems to verify their effectiveness. Simulate various failure scenarios to ensure that the recovery process works as expected.

9. Monitoring and Alerting:

Real-time Monitoring: Continuously monitor the health and status of both primary and remote systems. Set up alerts to notify administrators of any issues that may require attention.

10.Documentation:

Recovery Documentation: Maintain detailed documentation of recovery procedures, including step-by-step instructions and contact information for support personnel.

11.Regulatory Compliance:

Compliance with Regulations: Ensure that the remote recovery system adheres to any regulatory requirements governing data storage, privacy, and security.

Thank you .....