Resource Management-2 and Cloud Security – Revision Notes

Resource Management – Quick Revision

◇ **Objectives of Resource Management**

- **Scalability** – Handle increasing loads
- **Quality of Service (QoS)** – Maintain performance
- **Optimal Utility** – Efficient resource use
- **Reduced Overheads** – Lower operational costs
- **Improved Throughput** – More tasks completed per time
- **Reduced Latency** – Less delay
- **Specialized Environment** – Custom setups
- **Cost Effectiveness**
- **Simplified Interface**

◇ **Challenges (Hardware + Software)**

- CPU, Memory, Storage
- Network elements, Sensors/Actuators
- OS, APIs, Protocols
- **Energy consumption**
- **Load balancing**
- **Security**, **Delays**, **Bandwidth**

◇ **Aspects of Resource Management**

- **Provisioning**
- **Allocation**
- **Requirement Mapping**
- **Adaptation**
- **Discovery**
- **Brokering**
- **Estimation**
- **Modeling**

◇ **Performance Metrics**

- **Reliability**
- **Ease of Deployment**
- **QoS**
- **Delay**
- **Control Overhead**

Cloud Security – Quick Revision

◇ **Basic Components**

- **Confidentiality** – Data hidden from unauthorized access
- **Integrity** – Data correctness (authenticity + no tampering)
- **Availability** – Resources always accessible

◇ **Types of Security Attacks**

1. **Interruption** – Availability attack
2. **Interception** – Confidentiality breach
3. **Modification** – Integrity attack
4. **Fabrication** – Authenticity attack

◇ **Classes of Threats**

- **Disclosure** – Snooping
- **Deception** – Modification, spoofing, denial of receipt
- **Disruption** – Interrupting services
- **Usurpation** – Gaining unauthorized control

◇ **Operational Issues**

- **Cost-Benefit Analysis** – Prevention vs recovery
- **Risk Analysis** – What/How much to protect?
- **Legal & Cultural constraints**

◇ **Types of Attacks**

Passive Attacks – *No data alteration*

1. **Message content release**
2. **Traffic analysis**
   - ! *Hard to detect*

Active Attacks – *Involve data manipulation*

1. **Masquerade**
2. **Replay**
3. **Modification**
4. **Denial of Service (DoS)**

◇ **Common Attack Techniques**

- **Phishing/Social Engineering**

- **Password attacks**
- **Physical theft**
- **Command injection / Buffer overflow**
- **Backdoors / Packet fabrication**
- **DoS**
- **Exploitation of logic flaws**
- **Snooping**

◇ **Disaster Recovery Terminology**
- **RPO (Recovery Point Objective)**: Max data loss acceptable
- **RTO (Recovery Time Objective)**: Max time allowed to restore

◇ **Fault Tolerance Techniques**
- **Replication**: Mirroring data across multiple physical sites
- **Redundancy**: Duplicate critical components for backup/fail-safe