Mobile Computing

Mobile computing is a human-computer interaction in which a computer is expected to be transported during normal usage. It involves mobile communication, mobile hardware and mobile software. This allowes for the transmission of data, voice, and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. The term "mobile Computing" refers to a group of IT tools, Services, and operational methods that allow users to acess Computing, data and related resources and capabilities while on the go.

This is a technology that allowes anytime, anywhere 'OR' and everywhere computing.

i) Allows user to perform any task from anywhere using a compating device.

ii) communication is spread over both WIRED and WIRELESS media.

iii) Set of distributed computing systems participate, connect and synchronize through mobile communication procotocol.

iv)

Characteristics of Mobile computing :

- Portability - Devices / nodes connected within the mobile computing system should facilitate mobility
- connectivity - this defines the quality of service (QoS) of the network connectivity.
- Interactivity - The nodes belonging to a mobile computing system are connected with one another to communicate and collaborate through active transactions of data.
- Individuality - A portable device or a mobile node connected to a mobile network must have a unique identification number
- Content sensitivity - The ability to gather and respond to real or simulated data unique to a current location, environment, or time.

Applications of Mobile Computing

1- Healthcare Applications

Mobile health (m-Health) Solutions - Apps help (my Fitness pal) users track their diet and exercise.

2- Remote patient monitoring

3- Telemedicine

2- Business and Productivity

1) Mobile office Applications - Apps like Microsoft office and Google Workspace allow for document creation and Collaboration.

ii) Collaboration Tools - Platforms such as Slack and Zoom enhance team communication and facilitate meetings.

iii) Mobile CRM Systems - Apps like Salesforce and Hubspot help manage customer relationships on the go.

3- Education
4- Entertainment
5- Navigation
6- Emergency Services.
7- Logistics and Transportation
8- Retail
9- Personal communication
10- Agriculture
11- Environmental Monitoring
12- Manufacturing.

Benifits of Mobile Comp

1- Increased Productivity
2- Improved Efficiency
3- Enhanced Connectivity
4- Greater Accessibility
5- Personalization.

Examples - Smartphones, cloud etc.

Challanges of Mobile Computing

1- Security
2- Power consumption
3- connectivity
4- Data management.

Client-Server Architecture

Client-Server Architecture involves a client application (e.g. mobile application) requesting services or data from a server, which then processes the request and sends back a response. This architecture allows for efficient use of resources by offloading processing intensive tasks to the server while the client handles user interaction.

Key aspects of c/s architecture in mobile computing

Client : Initiates requests.

Server : This is the backend system that processes requests, manages data, and provides services.

Communication : client and server communicate over a network using protocols like HTTP or other specialized protocols.

Advantages

Resource optimization
Centralized Data management
Scalability
Security
Ex- Bank transaction through phone while charging
Reduced client complexity.

N-tier architecture

N-tier architecture commonly known as multi-tier architecture is a client-server architectural model that divides an application into multiple logical layers or physical tiers, each with a specific responsibility.

Layers vs. Tiers

Layers are logical separations of codes, while tiers are physical separations often running on different machines or even geographically separated locations.

Separation of Concerns

Each tier focuses on a specific aspect of the application, like presentation (user interface), business logic and data management, promoting modularity and reducing dependencies.

Client - Server Model

N-tier architecture commonly utilizes a client-server model, where clients request services from servers in other tiers.

Communication

Tiers communicate with each other through defined interfaces, often using protocols like HTTP or messaging queues, depending on the specific implementation.

Common Tiers in a 3-Tier Architecture

Presentation Layer (Client Tier)

Handles user interface and interactions displaying information and receiving user input.

Application Layer (Logic Tier)

Contains the business logic and rules, processing data and interacting with the data tier.

Data Tier (Database Tier)

- Manages data storage and retrival, interacting with the application tier to store and access information.

Benifits of N-tier Architecture

Scalability:

Individual tiers can be scaled independently to handle increased load, improving performance and resource utilization.

Flexibility:

Changes or updates to one tier don't necessarily require changes to other tiers, making the application more adaptable to changing requirements.

Maintainability

Separating concerns into distinct tiers simplifies code management, testing and debugging.

Security

N-tier architectures can enhance security by isolating sensitive data and logic within specific tiers, restricting acces from other tiers.

Reusability

Components within tiers can be reused across different applications or modules, reducing development time and efforts.

Uses:

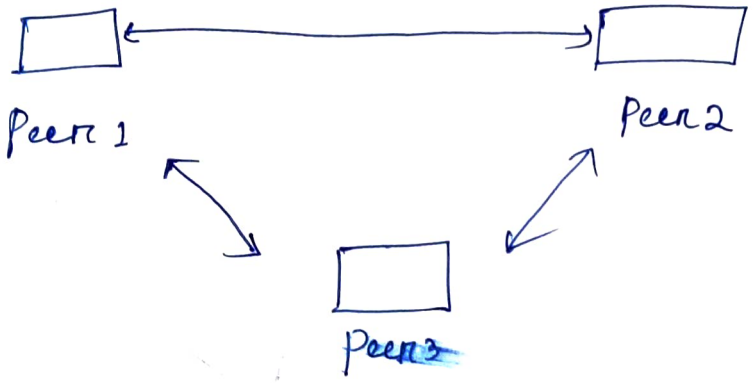
Large, complex applications requiring high scalability and maintainability. Applications with evolving business logic and frequent updates. When security is a primary concern and sensitive data needs to be isolated.

N-Tier Architecture

client and servers communicate through http. clients are the browsers which interpret the user interface in HTML and other client side scripting languages for rendering user interface. The servers are the web servers which serves the client request coming from HTTP with HTML response.

Peer-to-Peer Architecture

P2P/Peer-to-peer architecture is a type of network in which each workstation has equivalent capabilities and responsibilities.



Advantages

- No need of a network administrator
- Network is fast / inexpensive to setup and maintain
- Each PC can make backup copies of its data to other PCs for security.
- Easiest type of network to build, Peer-to peer is best suitable for home and office use.

Mobile agent architecture

Mobile agents have the following properties.

- They are the programme which hide data and code which are transported from client machine to remote server for execution
- They execute asynchronously

Mobile agents have no relation with mobile user, mobile device or any other aspects of mobility. They are software components which move from server to server in a network while keeping the state of applications intact.

Spread Spectrum

Spread spectrum is a technique used in wireless communication where a signal's bandwidth is deliberately broadened to make it more robust and secure. This is achieved by modulating the signal with a code that is wider than the original signal's bandwidth. By spreading the signal over a wider frequency range, spread spectrum methods enhance resistance to interference, jamming, and eavesdropping, while also improving bandwidth sharing and security.

Key Concepts

- Bandwidth Expansion
- Pseudorandom Codes.
- Processing gain
- Interference Resistance.
- Security

Types of Spread Spectrum.

1) Direct Sequence Spread spectrum (DSSS)

This method multiplies data signal by a pseudorandom code, effectively spreading the signal's energy across a wider bandwidth.

2) Frequency Hopping Spread spectrum (FHSS)

This rapidly switches the carrier frequency of the signal according to a pseudorandom sequence, hopping across a wide freq. band.

3) Time hopping Spread Spectrum

THSS transmits signal bursts in pseudorandom time slots within a frame, spreading the signal across time.

Advantages

Bluetooth, GPS, CDMA Cellular System.

DSS

This is a modulation technique that spreads a narrowband signal across a wider frequency band, making it more resistant to interference and jamming. It works by multiplying the data signal with a pseudorandom (PN) code, effectively "spreading" the signal over a wider spectrum.

Spreading the signal

DSSS achieves this spreading by multiplying the data signal with a higher-rate pseudorandom (PN) code. This PN code is a sequence of bits that appear random but are actually generated by a known algorithm, allowing the receiver to "despread" the signal.

Resistance to interference

By spreading the signal, DSSS makes it less vulnerable to narrowband interference. The interference affects only a small portion of the spread signal, making it easier for the receiver to recover the original data by despreading.

Enhance Security

The PN code acts as a form of encryption, making it difficult for unauthorized users to intercept or jam the signal. They would need to know the specific PN code used for transmission to decode the data.

Applications

DSSS is widely used in technologies like Wi-Fi, bluetooth, and GPS, where reliable and secure wireless communication is crucial.

Despreading at the receiver

The receiver uses the same PN code to multiply the received signal, effectively "compressing" the signal back to its original bandwidth, while also cancelling the noise.

FHSS

This stands for Frequency - Hopping Spread Spectrum. It's a method of transmitting radio signals by rapidly switching the carrier frequency among many frequencies within a wide band. The switching is controlled by a code known to both the transmitter and the receiver making it more robust to interference and jamming.

Working Principle

Instead of transmitting on a single, fixed frequency, FHSS systems hop between different frequencies according to a predetermined pattern. This pattern is known to both the transmitter and the receiver, allowing them to stay synchronized.

Robustness to interference and jamming

By hopping frequencies, FHSS makes it difficult for an interfering signal to disrupt the entire communication, as it only affects the signal during the short time it occupies a specific frequency.

Reduced interference

The hopping nature of FHSS also helps reduce interference with other users of the same frequency band, as the signal spends only a fraction of its time on any given frequency.

Security

FHSS can be used to enhance security, especially when combined with cryptographic techniques, making it harder for unauthorized parties to intercept or jam the signal.

Eg. • FHSS is used in military communications, where security and robustness are paramount.
• It is also used in Bluetooth technology, where it helps to maintain a reliable connection even in environments with many other wireless devices.
• Walkie-talkies also sometimes utilize FHSS for similar reasons.

FHSS can be implemented with different hopping rates. Fast FHSS involves hopping more frequently, while slow FHSS hops less often. The choice between them depends on the specific application and the desired level of robustness and security.

Cellular systems in mobile computing are categorized by generations, with each generation building upon the previous with improved technologies and capabilities. The primary types include 1G (analog), 2G (digital, including GSM and CDMA), 3G, 4G (LTE), and 5G.

Cellular System

A cellular system is a wireless communication technology that devides a large geographic area into smaller regions called cells, each served by a low power base station. This "cellular concept" allows for frequency reuse, enabling many mobile users to share limited radio frequency efficiently. Key components include mobile devices, base stations, and a central Mobile Telephone Switching Office (MTSO). As a mobile device moves between cells, it is handed off seamlessly to a new base station, ensuring continuous service.

Mechanism

1. Cell division

The overall service area is divided into hexagonal "cells", a theoretical shape that minimizes gaps and ensures consistent distance for radio signals.

2. Base stations

Low-power transmitters and receivers in each cell to communicate with mobile phones.

3. Switching centre

Handle call routing and manage connections between mobile phones and the broader public switched telephone network (PSTN).

Mobile Devices

Handheld units (phones) that contain transceivers to send and receive signals to/from the base stations.

Multiple Access Technologies

Methods like FDMA, TDMA and CDMA that allow many users to share the same wireless spectrum simultaneously.

How it works

1. Cellular Devices.
2. Mobile Connection.
3. Frequency Re-use.
4. Hand-off.
5. Network Connection.

Evolution of Cellular Technology

1G
2G
3G
4G
5G