

Unit I: Introduction: Mobile Computing – Networks – Middleware and Gateways – Application and Services (Contents) – Security in Mobile Computing. Mobile Computing Architecture: Architecture for Mobile Computing –Three-tier architecture – Design considerations for Mobile Computing.

CHAPTER 1

Mobile Computing Networks

1.Introduction of Mobile Computing

Mobile Computing is a technology that provides an environment that enables users to transmit data from one device to another device without the use of any physical link or cables.

mobile computing allows transmission of data, voice and video via a computer or any other wireless-enabled device without being connected to a fixed physical link. In this technology, data transmission is done wirelessly with the help of wireless devices such as mobiles, laptops etc.

This is only because of Mobile Computing technology that you can access and transmit data from any remote locations without being present there physically. Mobile computing technology provides a vast coverage diameter for communication. It is one of the fastest and most reliable sectors of the computing technology field.

The concept of Mobile Computing can be divided into three parts:

- Mobile Communication
- Mobile Hardware
- Mobile Software

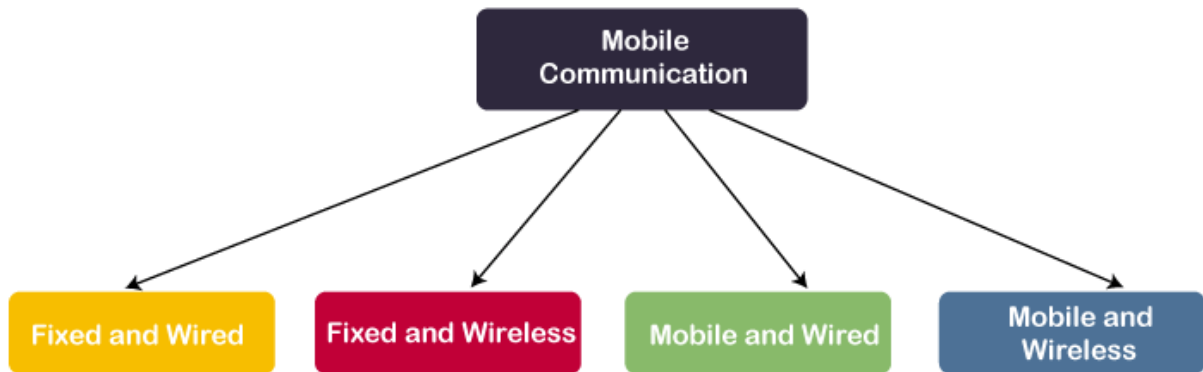
Mobile Communication

Mobile Communication specifies a framework that is responsible for the working of mobile computing technology. In this case, mobile communication refers to an infrastructure that ensures seamless and reliable communication among wireless devices. This framework ensures the consistency and reliability of communication between wireless devices. The mobile communication framework consists of communication devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services. These devices are responsible for delivering a smooth communication process.

Mobile communication can be divided in the following four types:

1. Fixed and Wired
2. Fixed and Wireless
3. Mobile and Wired

4. Mobile and Wireless



Fixed and Wired: In Fixed and Wired configuration, the devices are fixed at a position, and they are connected through a physical link to communicate with other devices.

For Example, Desktop Computer.

Fixed and Wireless: In Fixed and Wireless configuration, the devices are fixed at a position, and they are connected through a wireless link to make communication with other devices.

For Example, Communication Towers, WiFi router

Mobile and Wired: In Mobile and Wired configuration, some devices are wired, and some are mobile. They altogether make communication with other devices.

For Example, Laptops.

Mobile and Wireless: In Mobile and Wireless configuration, the devices can communicate with each other irrespective of their position. They can also connect to any network without the use of any wired device.

For Example, WiFi Dongle.

Mobile Hardware

Mobile hardware consists of mobile devices or device components that can be used to receive or access the service of mobility. Examples of mobile hardware can be smartphones, laptops, portable PCs, tablet PCs, Personal Digital Assistants, etc.

These devices are inbuilt with a receptor medium that can send and receive signals. These devices are capable of operating in full-duplex. It means they can send and receive signals at the same time. They don't have to wait until one device has finished communicating for the other device to initiate communications.

Mobile Software

Mobile software is a program that runs on mobile hardware. This is designed to deal capably with the characteristics and requirements of mobile applications. This is the operating system for the appliance of mobile devices. In other words, you can say it the heart of the mobile systems. This is an essential component that operates the mobile device.

This provides portability to mobile devices, which ensures wireless communication.

Applications of Mobile Computing

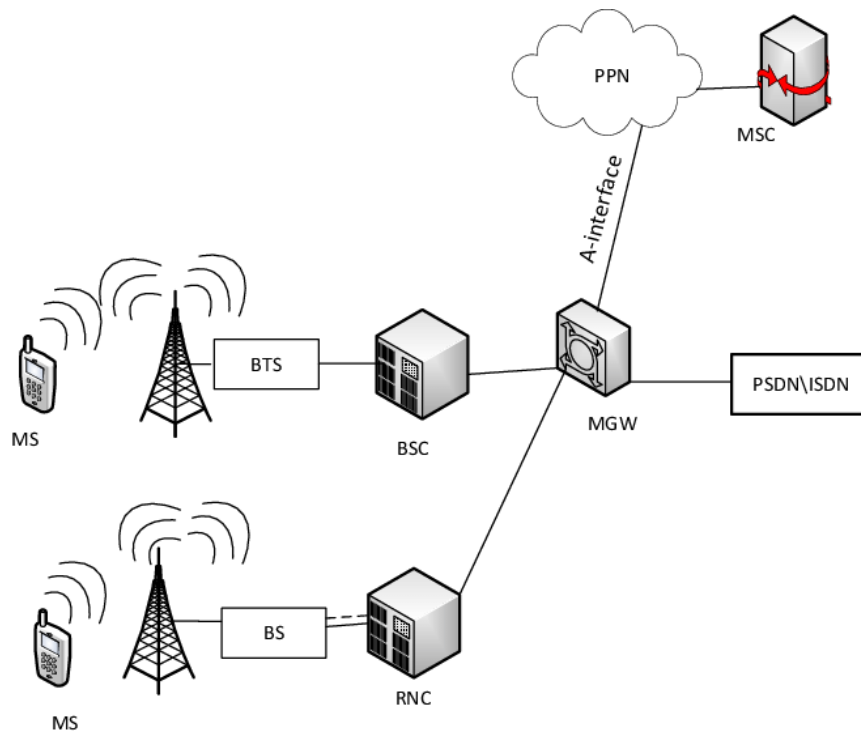
Following is a list of some significant fields in which mobile computing is generally applied:

- Web or Internet access.
- Global Position System (GPS).
- Emergency services.
- Entertainment services.
- Educational services.

1.2 Networks :

Mobile IP The following topic gives an overall view of Mobile IP, and the extensions needed for the internet to support the mobility of hosts. A good reference for the original standard is Perkins and Solomon which describe the development of mobile IP, all packet formats, mechanisms, discussions of the protocol and alternatives etc. in detail. The new version of Mobile IP does not involve major changes in the basic architecture but corrects some minor problems. 4.1.1 Goals, assumptions and requirement of mobile IP The main goal of mobile IP

is supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols. A host needs a topologically correct address to deliver a packet (mail boat). In a mobile state, the system will receive many packets. (i.e.) when the system leaves one network and joins another network, in transit the system receives many packets. All these packets need to be delivered correctly. A host sends an IP packet with the header and the message. The header contains a destination address. The role of the header is to determine,



1.3 Middleware :

What is Middleware?

Middleware is Software that provides a link between separate software applications. It is a layer that lies between the operating system and applications.

Use of Middleware:

- Provide interaction with another service or application.
- Filter data to make them friendly usable.
- Make an application independent from network services.
- Make an application reliable and always available.
- Add complementary attributes like semantics.

Types of Middleware:

1. Communication Middleware : Communication Middleware is used to connect one application with another application. For Example connecting one application with another application using telnet.

2. **Message Oriented Middleware:** It supports the receiving and sending of messages over distributed applications. It enables applications to be disbursed over various platforms. It makes the process of creating software applications across many operating systems. It makes network protocols less complicated. It holds many advantages over middleware alternatives and is one of the most widely used types of middleware.
3. **Object Oriented Middleware :** Object Oriented Middleware is also known as an object request broker. It provides the facility to send objects and request services via an object oriented system. In short, it manages the communication between objects.
4. **Remote Procedure Call (RPC) Middleware :** It provides the facility to calls procedures on remote systems and is used to perform synchronous or asynchronous interactions between applications or systems. It is usually utilized within a software application.
5. **Database Middleware:** It provides direct access to databases and direct interaction with databases, There are many database gateways and connectivity options and you simply have to see what will best work for your necessary solution. This is the most general and commonly known type of middleware. This includes SQL database software.
6. **Transaction Middleware :** This type of middleware includes applications like transaction processing monitors. It also encompasses web application servers, These types of middleware are becoming more and more common today.
7. **Embedded Middleware :** This type of middleware allows the facility of communication and integration of services with an interface of software or firmware. It acts as a liaison between embedded applications and the real time operating system,
8. **Content-Centric Middleware:** This type of middleware allows you to abstract specific content without worry of how it is obtained. This is done through a simple provide / consume abstraction. It is similar to publish / subscribe middleware, which is another type of this software that is often used as a part of web based applications.

Gateways

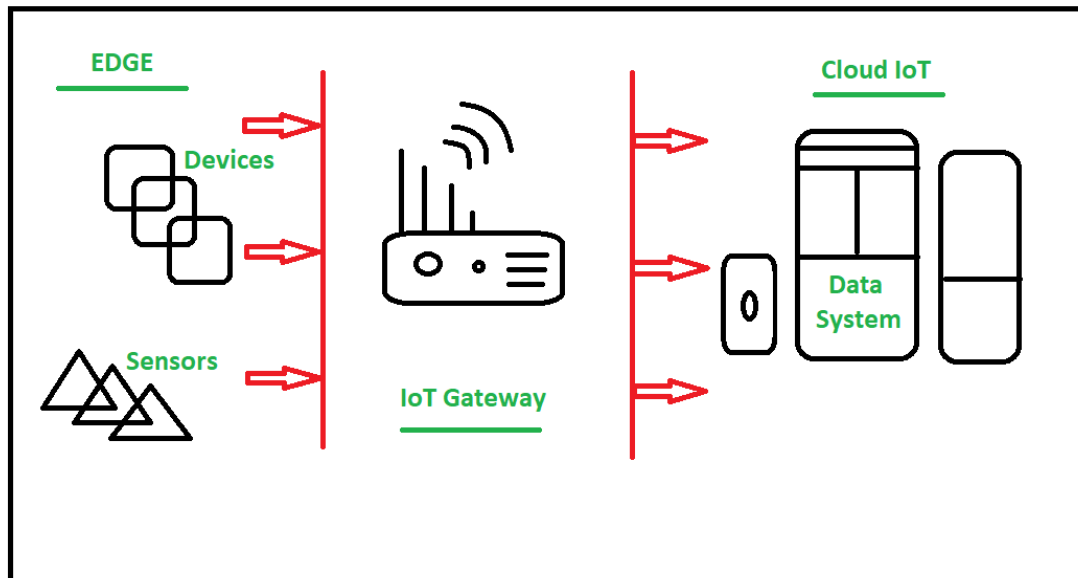
Gateways make communication between the application and the server feasible by connecting them altogether through a network tube, an imaginary tube that is believed to exist between the application and the server and constituted by network waves through which data transmission takes place.

A request about a certain amount of data is made by the user end and then the server finds and processes data accordingly with the request.

The transmission is made via network tubes through the server to the gateway and then the gateway to the application that made a request for data.

Gateways are considered to be the backbone for preserving the intelligence as well as the storage capacity of the Smart device altogether without compromising on the loss of the duo.

Gateways do this by application of Fog computing, on which a brief is provided below that helps you to get an overview of the deal between Gateways and Fog Computing and the whole data processing thing.



Why It Is Important to Learn About Gateways?

Gateway is not just hardware but a program in itself as important as other aspects of the Internet of Things. Gateways are designed as a passage for data transfer and the more intelligent a gateway could be, the more secure gateways could be, the more approachable the gateways could be, the more sophisticated the programming and designing of gateways could be, the more approachable and user-friendly internet of things be and the users could access and enjoy the smart objects in their life more easily.

If gateways could be understood and made in a manner that makes their potential, accessibility, and user-friendliness to the mark, there could be prominent growth and more security on the Internet of Things. For instance, think of a gateway connected to the smart refrigerator, so now all functions like requesting for data and sending data wherever needed could be done through the gateway itself, and if somebody could get access to the gateway he/she could steal, modify or hinder data. Also, if the gateway could be accessed without authority consent, it could be manipulated by a false server and data could be sent where it should not, and thus machine learning algorithms could verify all of it by various methods.

Features Of Gateways :

Gateways provide a wide variety of features. Some of which are:

Gateways work as a network bridge for data transmission as it makes the transmission of data possible to transmit with more ease and does not demand high storage capacity.

Gateways create a structural temporary storeroom for the data transmitted by the server and data requests made by the user end.

Gateways made the transmission more feasible as it queued up all the data and divide it into small packets of data rather than sending it bulk. Data transmitted through Gateway is divided into various useful and small packets each having its individual significance and a role to play while processing data.

Gateways made the data more secure if the modifications to the gateway could be done which then could create more reliability over smart devices.

Gateways optimize the data for search engines, applications, and servers by implanting better readability to the content so that a machine could understand and optimize data with ease.

Types Of Gateways :

There is not any specification of gateways in the commercial market other than being brand specific. But on the feasibility, performance, speed, and workability gateways can be classified in a broad manner as:

High Bandwidth Gateways –

These Gateways are meant for a more complex and intelligent Internet of Things or when there are lots of data to be processed and transmitted and a lot of smart devices to be handled once a time. These gateways could process data with more speed and flexibility and are able to handle more data at a time. Gateways basically are not categorized as such in the market, but various brands have certain specifications through which it could be decided either the gateway is of high bandwidth or not.

Low Bandwidth Gateway –

These Gateways are really the best choice while choosing a simple smart object or when you want to handle a single device once at a time. These Gateways are usually cheap and are easy going with simple smart devices, and usually need a sink* for more feasibility. They are really awesome if want a cheap solution to your data transmission.

Advantages Of Gateways :

The gateways provide the following advantages to the user:

It is possible through gateways that smart objects rely on fog computing for data transfer between user and server.

Gateways provide a way for the feasibility of smart objects without reducing the intelligence of objects as there is no need to transfer the intelligence of objects on the server-side hence preserving performance and accessibility

Gateways make the use of smart objects energy-efficient as data transfers do not rely on the smart device and transfers between devices and gateways are possible through low energy options like BLE, ZigBee, or Bluetooth.

Gateways open a new technology to the world, i.e., fog computing.

Gateways could add an extra layer of security to the data if certain modifications added to them.

Gateways make data encryption, data analysis, and handling possible so that a new phase of smart objects is available to users.

Gateways drive industries to innovate and make it possible for industries to grow more.

Gateways led industry and set up an employment opportunity as if development to gateways is made there are more people brainstorming to make gateways more feasible and overcome limitations.

1.4 Applications and Services :

As digital transformation continues to accelerate and reshape how the world conducts business, applications are taking on increased significance. Today, organizations large and small rely heavily on essential software solutions, not only to support and enhance, but to drive success. And this reliance on business software is only increasing.

But as innovation accelerates, concerns about application security, visibility, consistency, and performance are likewise becoming more pressing. After all, when software is central to a business, what happens when that software fails to perform optimally, efficiently, or securely?

In many cases, application services and application service management may be the answer. Application services support and enhance application use, configured to provide companies with specific software services. Application services are made up of applications and hosts that operate in tandem and may be designed either for business- or customer-facing app solutions.

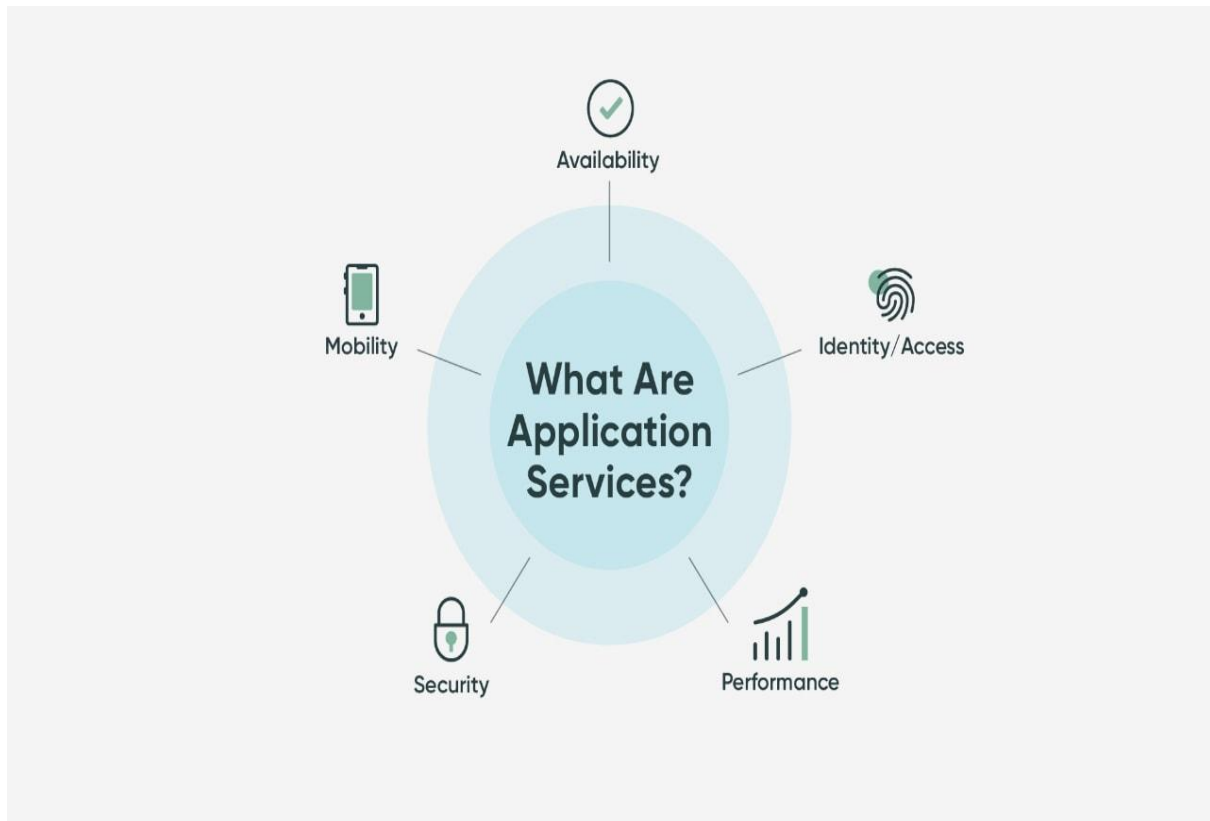
Why Application Services important ?

Modern businesses rely on an increasingly complex IT landscape. In fact, Okta reports that the average business organization currently deploys 89 distinct applications in 2022—an increase of 24% from 2016. This mix of application systems may include legacy technologies, software-as-a-service (SaaS) solutions, monitoring software, and more.

Unfortunately, supporting vital business applications and ensuring that the right governance solutions are in place is a massive responsibility—one that can easily consume the time, attention, and resources of existing IT departments.

Application services and related application service management solutions apply technology to take that responsibility off from the shoulders of beleaguered IT personnel. This empowers

IT professionals and the organizations that depend on them to apply more of their resources towards building strategy and driving business growth.



What are types of Application Services :

- There are applications to address almost any business need, the range of application services is likewise extensive. Even applications that are designed for simple and singular tasks require many support apps and hosts, all configured to provide the intended service. Consider, for example, what it takes to create a financial report using a web-based application: web servers, databases, application servers, network infrastructure, and middleware are all vital services that operate together to make the report a reality.
- Other examples of application services include credit card payment services, CRM systems, exchange rate services, online storefronts, order management systems, and inventory management systems.
- With that in mind, here are five categories of application services and several examples of each:

Access

Access application services are those that help verify user identity and enable access to secure applications, networks, platforms, etc. These services include:

- App access
- ID federation
- Secure web gateway
- SSL VPN
- SSO

Applications of Mobile Computing

There are different types of real life applications which are used in the Mobile computing, such as:

Traffic

- During traveling in traffic if we require to know road situation, latest news and when if feel more stress in driving then can play music and other important broadcast data are received through digital audio broadcasting(DAB). If we forget the road then we can know our exact location with the help of global positioning system (GPS).In case if got accident then can to inform police and ambulance via an emergency call to the service provider, which help to improve organization and save time & money.

Emergencies Situation

- To play a vital role in the medical sector can hire an ambulance with great quality wireless connection and help of this can carry significant information about injured persons. The useful step can prepare for a particular accident and doctor can be consulted for diagnosis. Only Wireless networks work of communication in nature disaster 2 such as earthquakes, tsunami, flood, and fire. In worst conditions only decentralized, wireless ad-hoc networks survive. Means that can handle Emergencies situation by mobile computing easily.

Use in Business

- As per business point of view CEO help of this computing system can represent the presentation at the front of their clients while can access hot news of the market. Help of video conference could be discuss at the topic without hindrance any time. Another side if traveling salesman wants to access the company database as per requirement then can be retrieved data on his wireless device and maintain the consistency company's database. Cause of these every employee are updated up to date.

Credit Card Verification

- Credit card verification using this computing most secure. In respect of Sale terminals(POS) when customer buy items in malls and other small shops when and pay bill in the form of swap credit card for transactions then need to establish network in between POS terminal and bank central computer then over protected cellular network verify the credential information of card Fastly.if match it then proceed

further otherwise denied get boost up speed of transaction process and relieve the burden at the POS network.

- Replacement of Fixed Networks
- Wired network has been replaced in wireless network e.g. trade shows, remote sensors and historical buildings. in wired networks, weather forecasting, earthquake detection and to get environmental data are impossible. This is possible only in adapting the replacement of fixed networks in this computing.

Infotainment

- Wireless networks are capable to deliver the latest information at any suitable regions and can download knowledge about concert at morning through wireless network that concert is conducting in any region as well as Another growing field of wireless network applications lies in entertainment and games to enable, e.g., ad-hoc gaming networks as soon as people meet to play together. So Infotainment by wireless computing is more easy.

Courts

- Defence counsels are able to take decision for using mobile computer in court. Whenever the opposing counsel are getting to reference a case that are not familiar, then they can implement to get direct, real-time access to on-line legal database service, where they can collect on the case and related precedents. So, mobile computers let instantly get access to a wealth of information and making person better informed and prepared.

Social Media Portal

- Few mobile applications let users to keep in get touch along with their friends and relatives by sending picture, audio, video, and text messages.
- To Collect Stock Information
- In such environment whereas to get access to stock is very limited like as factory warehouses. Therefore, with using of mobile computers, you can also get access the small electronic database. It also lets to data collate directly written to a central database through CDPD network, so it holds all stock information hence the need for getting to transfer of data to central computer at a later data is not mandatory.

E-Government

- Mobile computing concept is also using by governments to offer many services to get update their rural areas like as health, safety, farming, weather, education and other related information to governance. Therefore, government are getting to link rural areas along with head quarter offices for monitoring.
- Using in Organizations
- Head manager can also use mobile computers to prepare the critical presentation to valuable clients. They can also get access the latest market share data, and revise the presentation to take benefits of this information. They can also get communicate along with office about possible new offers and call meetings for discussing responding to new proposals.
- Tour and Travel

- Today, tourism is making a largest industry in pan world. Most of tourist spots are at remote location from the developed areas. Therefore with using of wireless communication, you can easily to connect for people who are joying their tour. They are easily to make connect along with family and relatives and finding out for travel service, hotel services food services and more.
- Transaction
- Few mobile applications let the facility of transaction like as pay bills, recharge mobile and so on.
- Paging & Electronic Mail
- With helping of mobile unit, you can easily to send and read emails for any small or large scale business or individual; it also let them to keep in get touch along with any colleagues as well as immediately development that may affect their work. To get access to internet, implementing mobile computing technology, provides the individual to have massive arrays of knowledge at their fingertips. With using of paging, you are also getting more intercommunication capability in between individuals and using of a single mobile computing device.

Replacement of Fixed Networks

Wired network has been replaced in wireless network e.g. trade shows, remote sensors and historical buildings. in wired networks, weather forecasting, earthquake detection and to get environmental data are impossible. This is possible only in adapting the replacement of fixed networks in this computing.

Infotainment

Wireless networks are capable to deliver the latest information at any suitable regions and can download knowledge about concert at morning through wireless network that concert is conducting in any region as well as Another growing field of wireless network applications lies in entertainment and games to enable, e.g., ad-hoc gaming networks as soon as people meet to play together. So Infotainment by wireless computing is more easy.

Paging & Electronic Mail

With helping of mobile unit, you can easily to send and read emails for any small or large scale business or individual; it also let them to keep in get touch along with any colleagues as well as immediately development that may affect their work. To get access to internet, implementing mobile computing technology, provides the individual to have massive arrays of knowledge at their fingertips. With using of paging, you are also getting more intercommunication capability in between individuals and using of a single mobile computing device.

1.5 Security in Mobile computing :

Two types attacks are existed in the Mobile Computing security:-

Passive attack – In this attack intruder only monitor the transmitted data over the network.

Active attack – In which intruder gives some modification in the original data.

Concern Security is:

- Encrypted data
- Outsource detection
- Lack of data capacity
- Terminal tracer
- Set up timeout system
- Use reliable sources such as Google Play and Amazon App

What is mobile security (wireless security)?

Mobile security is the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.

Why is mobile security important?

- Securing mobile devices has become increasingly important as the number of devices and the ways those devices are used have expanded dramatically. In the enterprise, this is particularly problematic when employee-owned devices connect to the corporate network.
- Without mobile device security measures, organizations can be vulnerable to malicious software, data leakage and other mobile threats. Security breaches can cause widespread disruptions in the business, including complicating IT operations and affecting user productivity if systems must shut down.
- A lack of mobile security can lead to compromised employee, business or customer data. If an employee leaves a tablet or smartphone in a taxi or at a restaurant, for example, sensitive data, such as customer information or corporate intellectual property, can be put at risk.

How does mobile security work?

- As is the case with securing desktop PCs or network servers, there is no one single thing that an organization does to ensure mobile device security. Most organizations take a layered approach to security, while also adapting longstanding endpoint security best practices.
- Some of these best practices pertain to the way the device itself is configured, but other best practices have more to do with the way the user uses the device.

What are the benefits of mobile security?

- The most obvious benefit to mobile security is preventing sensitive data from being leaked or stolen. Another important benefit, however, is that by diligently adhering to security best practices, an organization may be able to prevent ransomware attacks that target mobile devices.
- At a higher level, a solid mobile device security plan can help to ensure regulatory compliance. A strategy also makes mobile devices and the software that runs on them easier to manage.

What are the challenges of mobile security?

One of the biggest challenges to mobile device security is the sheer variety of devices that employees potentially use. There are countless makes and models of smartphones, tablets and other mobile devices. Mobile device management (MDM) software generally supports the more popular devices and the latest mobile OSes, but not all security policy settings work on all devices.

Another challenge to mobile device security is the constantly evolving threat landscape. At one time, there were relatively few mobile threats for organizations to worry about. As devices became more widely adopted, however, cybercriminals began increasingly targeting mobile platforms.

What are the types of mobile device security?

Mobile device security often centers around the use of MDM. MDM capabilities are often available in enterprise mobility management and unified endpoint management tools, which evolved from the early device-only management options.

However, organizations typically use other security tools to enhance their mobile device security. This might include VPNs, antimalware software, email security tools that are designed to block phishing attacks and endpoint protection tools that monitor devices for malicious activity.

Mobile device security vendors and products

There are several vendors that offer mobile device management and security tools. Some of the tools available include:

- Scalefusion
- Hexnode Unified Endpoint Management
- Microsoft Enterprise Mobility + Security
- VMware Workspace ONE Unified Endpoint Management
- Google Endpoint Management
- N-able Remote Monitoring and Management

CHAPTER 2

Mobile Computing Architecture

2.1 Mobile Computing Architecture:

- This architecture represents the blueprint about the multiple layers in between network hardware components, devices and user application interface. Well – establish architecture is required for getting to access data, systematic calculations and software objects as well.
- Mobile Computing: Mobile computing is wireless technology that lets you to broadcast the data, video, and audio through devices which are not attached along with any physical medium. The main feature of mobile computing is that all computing devices are portable nature and linked over a computer network.

2.2 3-Tier Architecture of Mobile Computing

Mobile computing is enabled with three-tier architecture that has three major layers, so here we will explore each one layer with its functions; below shown all:

Also Read: [What is Green Computing with its Advantages, Disadvantages, and Examples!!](#)

Mobile Computing Architecture Layers:

- Presentation Layer (UI): This layer lets users to face device handling and rendering.
- Application Layer (AL): It allows executing business logic and rules.
- Data Access Layer (DM): It lets to get access and management.

1-Tier Presentation Layer

- This presentation layer lets to execute all applications on the client devices and provide complete user interfaces.
- It has main responsibility is to present information to edge-user.
- Users are able to grab all information via speakers, vibration, screens, etc.
- Users can sent the information with helping of input devices like pen drives, mouse, keyboard, touch screens and so on.
- This layer is enabled with WAP browsers, customized client programs, web browsers, etc.
- Presentation layer allows accomplishing via client-side data source, Dynamic HTML and data cursors.
- Presentation layer must be context aware and device-independent.

2-Tier Application Layer

- In the application layer, business logic performs all tasks as server for client requests from workstations. It works as business rules fetch or enter data through the Data Layer.
- It is enabled with few technologies such as PHP, .Net services, JSP, Java and so on.

- Presentation and database-independent
- This layer identifies that which types of data is required and performs as client in relation to a third tier or programming that may be situated on a mainframe computer or locally.
- It takes decision on rendering, network management, security, data store access, need for many types of middlewares.
- Their components are not linked to certain client, so they can be implemented by all applications and can be proceed to other locations, as responding time frame and other needed rules.

3-Tier Data Access Layer

This layer is implemented to keep store data that is required by application and work as repository for both temporary and permanent data.

- Data access layer is built up of DBMS that offers all data for above two layers.
- This layer is also known as ‘DBMS Access Layer’
- All data is stored into many format like as text files or relational DB.
- In this layer, to ignore the dependencies on the storage mechanism offers for getting to update or change without the application tier clients that is affected by aware of change.

2.3 Design considerations for mobile computing

- The mobile computing environment is constrained in many ways. Mobile elements themselves are resource-poor and unreliable. Their network connectivity is often achieved through low-bandwidth wireless links.
- These severe restrictions have a great impact on the design and structure of mobile computing applications and motivate the development of new computing models.
- These mobile computing models must provide efficient access to both existing and new applications which is a key requirement for the wide acceptance of mobile computing.
- An important design consideration is the type of functionality assigned to mobile hosts. Mobile units are still characterized as unreliable and prone to hard failures, i.e., theft, loss or accidental damage.

Thus following requirements must be considered for mobile computing environment:

1. Type of Application (Native or Mobile Web) :

- Before designing mobile application you need to determine type of application.
- If your application requires local processing. access to local resources than consider designing a native application.
- A native application is hard to maintain. requires separate distribution and upgrade infrastructure, are compatible only with target device/platform, requires more effort (sometimes huge) to port on different devices.
- A mobile web application is compatible with all devices with internet connection and a browser

2 Target device :

- Target device and platform (OS) plays a key role throughout design decisions making process.
- Design decisions are influenced by target device's screen size, resolution, orientations, memory, CPU performance characteristics. Operating systems capabilities, device hardware, user input mechanism (touch/non-touch), sensors (such as GPS or accelerometer etc).

3 User experience:

- User interface should be rich, intuitive and responsive. While using mobile application user is often distracted by external or internal (e.g. incoming call when user is in middle of a wizard) events. These events have to be factored in design.
- Screens should be identified with consideration that user is often focused on discrete individual task. Long data entry forms may irritate user and should ask for absolutely required data/information.

4 Resource Constraint:

- Every design decision should take into account the limited CPU, memory and battery life. Reading and writing to memory, wireless connections, specialized hardware, and processor speed all have an impact on the overall power usage.
- One cannot afford a long running process in application.
- In some cases, application processing should be offloaded from the device to avoid excessive resource consumption e.g. using notification or app directed SMS instead of polling to monitor a value/flag on server.

5 Multiple Platforms:

- There is high technology fragmentation in Mobile world. It is very unlikely that an application will target only one platform or only one device. In near future, requirement like same code base should support iPhone and iPad or Android Phone and Android tablet will arise. Architect should consider portability as important architectural goal.
- If you are developing for more than one device, design first for the subset of functionality that exists on all of the devices, and then customize for device-specific features when they are detected.

6. Security:

- Devices are more vulnerable than desktop, primarily due to lack of awareness. Moreover device can be lost easily. Ensure that the device – server communication is secured and server accepts request only from authentic source (device).
- If you are storing any confidential application or configuration data locally. ensure that the data is encrypted.

7.Network Communication:

Network communication on device is slow and costly. Reduce network traffic by combining several commands in one request e.g. committing added, updated and deleted record in one request instead of firing separate request on each add/update/delete.

Compress large text / XML data to lesser network traffic. Design for asynchronous communication.

Mobile elements are also resource poor relative to static hosts. For these reasons, there are approaches that treat the mobile unit as a dumb terminal running just a user-interface.

Besides the partition of data and computation of mobile applications between mobile and static elements, two important considerations in designing software system for mobile computing are: what is an appropriate model for mobile computing systems, and whether mobility should be made transparent to applications.